Definition der DESY Netzwerk-Bereiche

D4, NOC

v0.12, 05.06.2025

1 Internet und externe Netze

Als extern sind alle Netze außerhalb der DESY-Perimeter-Firewall "fw-wan" eingestuft. Auch das DESY-Gästenetz, eduroam sowie die Netze der StartUps hierzu.
Folgende bei DESY verwendeten Präfixe sind grundsätzlich als extern anzunehmen und daher vergleichbar zum Internet zu behandeln:

- 192.76.172.0/24
- 10.12.0.0/16
- 2001:638:700:e191::/64
- + N.N. "Zeuthener Gästenetz"
- + N.N. "Zeuthener eduroam"

Mögliche Zugriffe aus diesen Subnetz-Bereichen in die internen Netze können weniger Einschränkungen unterliegen als Zugriffe aus dem Internet, jedoch müssen Zugriffe in die DMZ und ins interne Netz in jedem Fall vorher mit D4 abgesprochen werden.

1.1 Partner-DMZ Netzwerke

Ein Teil des privaten 10.12.0.0/16 Subnetzes wird dafür verwendet, dass Gruppen anderer Institute ein Netzwerk verwenden können, dass es ihnen erlaubt, dichter an ihrem Heimatinstitut arbeiten zu können. Es ist in diesen Netzwerken sogar zulässig, dass dauerhafte site-to-site VPN Tunnel eingerichtet werden, so dass die Rechner bspw. in die Management-Infrastruktur des Heimatinstituts eingebunden sein könnten. Aus diesem Grund sind die Netzwerke der Partner-DMZ in der VRF extern und müssen wie Verkehr aus dem Internet durch die "fw-wan". Allerdings werden für diese Netzwerke Basisdienst wie z.B. Drucken eher freigeschaltet als für das Internet, da die Partner-DMZ nur für tatsächliche Partner-Institute eingerichtet werden. Die Clients werden auf eine Adresse aus dem externen Subnetz 192.76.172.0/24 geNATed, wenn sie eine Verbindung ins Internet aufbauen wollen. Die Möglichkeit einer Freischaltung von Services, um diese aus dem Internet erreichbar machen zu können, besteht nicht.
Derzeit haben

- HZI

- HZDR

eine Partner-DMZ eingerichtet bekommen.

2 DMZ

Die DMZ beherbergt Server, die Dienste anbieten, die in der Regel vom Internet aus erreichbar sein sollen und somit Freischaltungen in der Firewall erhalten müssen. Die DMZ bei DESY ist wiederum in mehrere Zonen unterteilt (vpnDMZ, SciDMZ, DMZ, ...), die aber hinsichtlich der Zugriffs-Regeln grundsätzlich alle gleich zu behandeln sind.
Alle Freischaltung auf Dienste in der DMZ aus externen Netzen und dem Internet müssen zuvor in einem Ticket bei D4 abgeklärt und im Freischaltungsformular beantragt werden. Nach Genehmigung erfolgt der Auftrag zur Einrichtung der Freischaltung durch D4 an NOC, direkte Anfragen werden abgelehnt und an D4 verwiesen. Freischaltungen von der DMZ in interne Netzwerke kann NOC ohne zwingende Beteiligung von D4 abwägen und ggf. einrichten.

3 Fernzugriff / VPN

Es gibt derzeit zwei bei DESY verwendete VPN Gateways, wobei zukünftig nur noch "eduVPN" den Standard-Fernzugriff auf das interne Netz darstellen wird.
Grundsätzlich sind die VPN-Netze als intern zu betrachten, alle Dienste, die von "jedem" Rechner auf dem Campus erreicht werden können, können auch aus dem eduVPN erreichbar sein. Da DESY i.d.R. jedoch keine Kontrolle über die verwendeten Endgeräte und insbesondere deren Betriebssystem-Version und Patchlevel hat, ist der Zugriff auf die in 3.2 genannten Ports begrenzt. Das Ergänzen zusätzlicher Ports kann bei D4 beantragt und vom Rechnersicherheitsrat (RSR) entschieden werden.

3.1 Cisco VPN

Das Cisco VPN nutzt den IP Adressbereich

- 131.169.252.0/22

der wiederum in Bereiche für den Standard-VPN Zugang (wird durch eduVPN abgelöst) und besonders privilegierte Zugänge mit wenigen Nutzerinnen und Nutzern aufgeteilt ist.

3.2 eduVPN

eduVPN ist eine auf wireguard basierende VPN-User-Portal-Lösung, die eine komfortable VPN-Verbindung mit MFA-Authentifizierung (DESY Keycloak) für alle Nutzerinnen und Nutzer mit primärem DESY Account bereitstellt.
Im eduVPN werden interne Subnetze aus dem IP Addressbereich

- 10.252.0.0/16
- 2001:638:700:e000::/52 (exkl. eduroam IPv6 Bereich, s.o.)

verwendet, ins Internet wird der Verkehr auf die öffentliche Adressen aus den Bereichen

- 131.169.10.192/27
- 2001:638:700:113b::/64

geNATed.
Aus dem eduVPN Netzen sind die gleichen Dienste wie nach einem 2FA ssh login auf 'bastion' erreichbar, neben Standard-Diensten (DNS, ldap, kerberos, Softphones...) insbesondere alle internen Dienste auf den Ports

- http(s)
- ssh
- rdp

insofern diese nicht durch weitere interne ACLs (vor zusätzlich gefirewallten Netzen, vor Kontrollnetzen, ...) eingeschränkt sind.

4 Intranet

4.1 Öffentliche IP-Adressen

DESY hat zwei Standorte, Hamburg (DESY-HH) und Zeuthen (DESY-ZN). Grundsätzlich sind alle öffentlichen wie privaten Netze von allen Rechnern im internen Netz von DESY erreichbar.
Hamburg und Zeuthen verwenden jeweils eigene öffentliche IPv4 Präfixe, die nur an dem jeweiligen Standort Verwendung finden. Der IPv6 Präfix ist aufgeteilt und ein "/52"-Subnetz-Bereich wird exklusiv in Zeuthen verwendet:

Hamburg:

- 131.169.0.0/16
- 2001:638:700::/48 (ohne Zeuthener IPv6 Bereich)

Zeuthen:

- 141.34.0.0/16
- 2001:638:700::f/52

Subnetze aus diesen Bereichen die oben als ëxternäufgelistet sind, sind nicht als Teil des Intranets zu betrachten.

4.2 Private IP-Adressen

Es werden private IP-Adressen aus den IP-Adressbereichen

- 192.168.0.0/16
- 10.0.0.0/8

verwendet. Intern (inkl. Zeuthen) können die IP-Adressen identisch zu öffentlichen IP-Adressen verwendet werden. Allerdings ist ein Internetzugang für diese privaten Adressen nicht ohne weiteres möglich, da am Perimeter kein NATing stattfindet. Sollte Bedarf an Zugang zu einzelnen Diensten im Internet (Updates, ...) bestehen, wenden Sie sich bitte an NOC.
Wir erwarten, dass die Verwendung von privaten Adress-Bereichen immer in Absprache mit NOC erfolgt, um die doppelte Verwendung und Adress-Konflikte zu vermeiden. Wir empfehlen, dies auch dann zu tun, wenn ein Netzwerk (zunächst) nur isoliert und nicht geroutet verwendet wird. Sollte es zu Konflikten kommen, kann nur die Gruppe ihren Adressbereich weiter verwenden, die diesen zuvor mit NOC abgestimmt hat. Alle anderen müssen dann ihre Konfiguration ändern.
Zeuthen verwendet nahezu ausschließlich öffentliche IP-Adressen, der IP-Addressbereich

- 192.168.224.0/19

ist für Zeuthen reserviert und wird in Hamburg nicht vergeben.
Subnetze aus diesen Bereichen die oben als ëxternäufgelistet sind, sind nicht als Teil des Intranets zu betrachten. Der Bereich 10.12.0.0/16 wird exklusiv für externe Dienste verwendet und ist daher nicht als intern zu betrachten.

4.3 “Wolken“ im Intranet

Das interne Netzwerk in Hamburg ist in drei Bereiche aufgeteilt, die jeweils auf eigener Hardware geroutet werden und durch ACLs (Access Control Lists) segmentiert sind:

4.3.1 Office-Netzwerk

- Netzwerk für die Büroarbeitsplätze, Drucker, Telefone, ...
- Geräte mit Zugang zum Office-Netz müssen durch Segment-Administratoren registriert sein und die Anforderungen des RSR erfüllen.
- Auf dem gesamten Campus verfügbar, VLANs werden für registrierte Geräte dynamisch zugewiesen.
- Standardmäßig ist jede linke Netzwerkdose auf dem Campus für einen dynamischen Zugang zum Office-Netz freigeschaltet.
- einige besondere Office-Netzwerke (Netze im V-Bereich, SAVE, ...) sind durch eine zusätzliche interne Firewall gesichert.
- Das Office-Netz hat zwei Äußenstellenïn Bonn und Uetersen, die mit einem site-to-site-VPN-Tunnel ans DESY Intranet angebunden sind

4.3.2 Rechenzentrums-Netzwerk

- Netzwerk für die Server in den DESY-Rechenzentren
- Registrierung von Geräten erfolgt nur durch IT

4.3.3 Kontroll-Netzwerke

Um einen möglichst sicheren, störungsfreien und unabhängigen Betrieb der Beschleuniger und der Experiment-Datennahme zu gewährleisten, werden die dafür erforderlichen Komponenten in Netzwerken betrieben, die jeweils auf eigener Hardware geroutet werden.
Vom Büro- und Rechenzentrumsnetzwerk unabhängige Kontroll-Netzwerke werden betrieben für

- Kryogenik (KRY)
- Petra (MCS)
- Petra-Datennahme (PDAQ, im Aufbau)
- Flash (FLASH)
- XFEL "Bahrenfeld $\rightleftharpoons$ Osdorf" (XACC)
- XFEL "Osdorf $\rightleftharpoons$ Schenefeld" (XDAQ)
- Kaldera (KLL)

Änderungen und Arbeiten an den Kontroll-Netzwerken erfordern besondere Vorsicht, um den Betrieb und die Datennahme nicht zu stören. Alle Arbeiten sowie Änderungen an den ACLs müssen mit den Netzwerk-/IT-Verantwortlichen des jeweiligen Beschleunigers abgestimmt werden.

5 Tabellarische Übersicht

Tabelle 1: Übersicht der Zugriffe zwischen den Netzwerk-Bereichen bei DESY, wobei grüne Felder grundsätzlich erlaubte Verbindungen, gelbe mit D4 bzw. den Maschinen-Veranwortlichen abzustimmende Verbindungen und rote nicht erlaubte/mögliche Verbindungen darstellen.