Grid-Anforderungen an Firewalls

Ein Statusüberblick und Ausblick

17. März 2009 | Ralph Niederberger und Egon Grünter

Überblick

- Einleitung
- Grid-Computing und Anwendungsszenarien
- Verfügbare Grid-spezifische Firewall-Lösungen
- Dynamische Freischaltungen
- Kurz-, Mittel und Langfristige Lösungen
  - Vom FTP zum FiTP
  - Status der Arbeiten
- Zusammenfassung und Ausblick

Einleitung

- Bedarf an Ressourcen für Forschung seit langem bekannt
- Beispiele für Ressourcen: Rechnerknoten, Speicherplatz, medizinische und physikalische Großgeräte, wie LHC, ITER
- Grids erlauben Nutzung dieser Ressourcen vor Ort oder remote
- sicherer und ausschließlich autorisierter Zugriff unabdingbar
- Zugriffssicherung gewährleistet durch Firewalls
- Große Komplexität der verwendeten Anwendungen
- Dynamische Schaffung, Veränderung und Auflösung von VOs

➢ Neue Aufgabenstellung für Firewall-Systeme

Vortrag gibt Überblick über neue Aufgabenstellungen, existierende Lösungsansätze & zukünftige Entwicklungen

Einleitung – Ausgangspunkt (1)

- Untersuchungen im D-Grid Integrationsprojekt 1 Fachgebiet 3 „Netze und Sicherheit – Firewalls“
  - Gridnutzer-Befragung über die von Firewalls in Grid-Umgebungen benötigten Funktionen
  - Performance und dynamische Konfiguration von Firewalls
  - Empfehlungen für die statische Konfiguration in den D-Grid Communities
  - langfristig tragfähige Ansätze zur dynamischen Konfiguration von Firewalls

- Nachfolgeprojekt D-Grid Integrationsprojekt 2 Fachgebiet 3.3 „Sicherheit“ Arbeitspunkt 2 „Dynamische Konfiguration“
  - weitergehende Analyse existierender Ansätze
  - prototypische Implementierung
  - Mitarbeit bei der Standardisierung zur dynamischen Freischaltung von Firewalls

Bundesministerium für Bildung und Forschung

Teilweise gefördert durch

DFN Deutsches Forschungsnetz

Einleitung - Ausgangspunkt (2)

- „Firewall-Issues Research Group“ des Open Grid Forum
  - Problemstellungen von Grids und Lösungen
  - Dokumente:
    - „Firewall issues overview“ GFD-083
    - „Requirements on operating Grids in firewalled Environments“ GFD-142
    - Mitarbeiter des Fachgebiet 3 aktiv seit Gründung der RG

- „Firewall Virtualization for Grid Applications Working Group“
  - Neue Arbeitsgruppe der OGF
  - Protokoll für die dynamische Freischaltung von Ports auf Firewalls für Grid-Anwendungen
  - Prototypische Implementierung
  - Ziel: Freischaltung ohne manuelle Interaktion von Firewall-Administratoren durch die Grid-Anwendung mittels üblicher AAA-Verfahren

Grid Computing

- Vision: Anwendungen haben on-demand freien Zugriff auf im Internet verteilte, durch andere Organisationen verwaltete, Ressourcen
- Dynamische Virtuelle Organisationen
- Anwendungs-gesteuerte Transport-Privilegien im Netz
- Vordefinierte Sicherheits-Policies im Netz
  (Firewalls, NAT, ALG, VPN-GW)
- Administration erfordert manuelle Konfiguration
- Ressourcen-Verteilung im Grid über Metascheduler
- Wissenschaftler weiß nicht, auf welche Ressourcen er zugreift, wem sie gehören, oder wer sie betreut
- nicht jeder Anbieter stellt seine Ressourcen weltweit zur Verfügung
- Zugriffsregelung durch Firewalls

Grid Anwendungsszenarien im Überblick (1)

- Globus Toolkit (Version 4)
  - Unterschiedliche Sicherheitslösungen etabliert
  - Job Start, Überwachung und Löschung
  - Zugriff auf Grid-Ressourcen und Daten
  - Kommunikation findet statt zwischen:
    - *Dynamische Client- zu festen Server-Ports (klassisches Client-Server-Konzept)*
    - *Dynamische Client- und Server-Ports (Portbereiche)*
    - *Dynamische Ports bei Clients und Portbereich bei Server(n)*
      ►schwer händelbar, da Ports je nach Anwendung unterschiedlich. Festlegung bei Programmstart.
  - Prominentes Beispiel für GTK Anwendung ist GridFTP
    - *aus FTP-Protokoll entstanden*
    - *erlaubt Kontrollverbindung (Port 2811) + mehrere parallele Datenverbindungen (dynamische Ports)*
    - *Meist im Vorhinein freigeschaltet*
    - *Third Party-File-Transfers*

Grid Anwendungsszenarien im Überblick (2)

- UNICORE (UNiform Interface to COmputing REsources)
  - Bietet über GUI einfachen, einheitlichen und sicheren Zugriff auf verteilte Computing Ressourcen
  - nutzt striktes Authentisierungs- und Autorisierungs-Schema, Plattform-Unterschiede versteckt
  - Besteht aus Client-Anwendung (GUI), Gateway und NJS/TSI (Network Job Supervior/Target System Interface)
  - NJS erzeugt aus abstrakt definiertem Job-Code Job-Statements für Ziel-System
  - Benutzer Authentisierung erfolgt mittels X.509 Zertifikaten
  - Gateway kann je nach Sicherheitsrichtlinie innerhalb und außerhalb von DMZs installiert werden
  - Gesamte Kommunikation über vordefinierten Port -> einfach für Firewall

Grid Anwendungsszenarien im Überblick (3)

- AccessGrid
  - Group Collaboration System zur Kommunikation verteilter Gruppen über das Internet
  - Ressourcen: Großbildwände, Video-Konferenz-Systeme, Präsentations- und Interaktionsumgebungen
  - Software in Grid-Umgebungen weit verbreitet
  - Kommunikation in virtuellen Meetings geschieht über teilweise parallele Multicast-Verbindungen
  - Da viele Firewalls Multicast nicht unterstützen muss die Kommunikation meist über Bypass oder Tunnel realisiert werden

Grid Anwendungsszenarien im Überblick (4)

- Hochgeschwindigkeits- und Weitverkehrs-Kommunikation
  - Grid Anwendungen benötigen häufig Hochgeschwindigkeitsnetze
  - U.A. auch TCP-Varianten, die im “normalen” Internet zu Unfairness zwischen Kommunikationsströmen führen
  - Daher oft auf dedizierten Netzen realisiert
  - Sicherung über Firewalls
  - Signalisierung derartiger Hochgeschwindigkeits-datenströme, d.h. das sichere Rerouting über alternative schnelle Pfade, z.B. durch Token derzeit von Firewalls nicht adressiert.

Klassifizierung der Grid-Anwendungen

reine Klassen, oft Mischformen vorhanden

- Anwendungen mit allgemein bekannten vordefinierten festen Ports (UDP oder TCP), wie EMail, SCP oder http.
  - Lösung: Freischaltung der well-known Ports
- Anwendungen mit in der Anwendung vorkonfigurierbaren Ports (Default-Ports bekannt)
  - Lösung: Beantragung der Freischaltung.
    Nachteil: Ports ständig offen, auch wenn Anwendung nicht läuft
- Hochgeschwindigkeitsübertragungen über dedizierte Hochgeschwindigkeitsnetze (vorgegebene Ports)
  - Lösung: Freischaltung auf Hochgeschwindigkeits-Firewalls.
    Nachteil: teuer und meist nur zeitversetzt am Markt verfügbar
- Dynamische Protokolle, z.B. FTP, SIP oder H.323
  - Lösung: Kauf einer Firewall, die diese Protokolle unterstützt
- Spezialisierte dynamische Protokolle, wie GridFTP
  - Lösung: Ständige Öffnung der vordefinierten Portbereich

Verfügbare Firewall–Entwicklungen für Grids

- Grundsätzliche Problem seit langem bekannt
- Daher bereits frühzeitig Erweiterungen in Firewall-Systeme eingeführt, wie für FTP, SIP und H.323
- Leider nicht für Grid-Anwendungen nutzbar, da eigene Grid-Protokoll-Standards genutzt werden
- Wegen geringer Verbreitung nicht in Firewall-Systemen integriert

- Einige Speziallösungen existieren für Firewall-Systemen, meist Linux-basiert

Speziallösungen: High Speed Firewalls

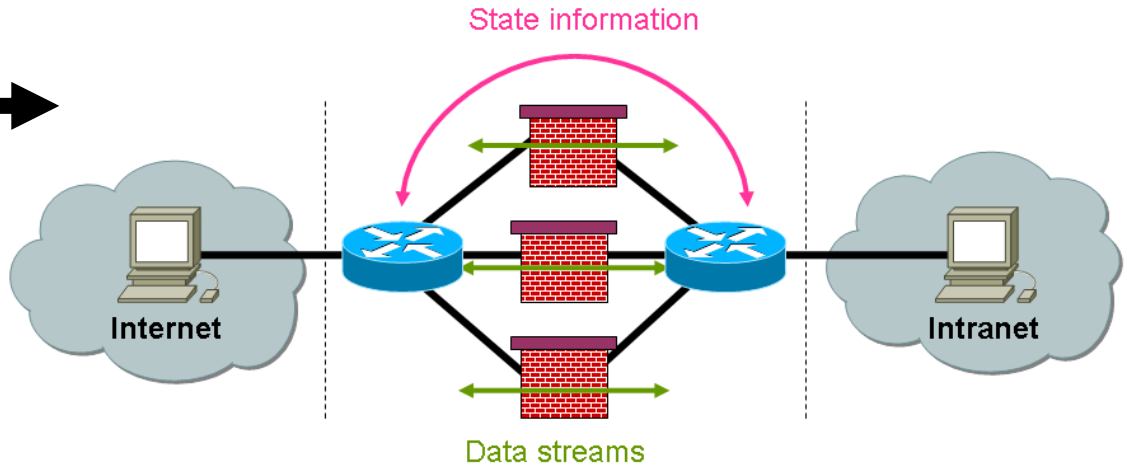
- Hochgeschwindigkeits-Firewalls mit Geschwindigkeiten bis mehreren 10 Gb/s verfügbar
  - Beispiele: Juniper Netscreen, Cisco ASA (Jumbo Frames)
- Aber teuer
- Durch Kauf eines weiteren Systems kann Ausfallsicherheit erreicht werden (Verdoppelung der Kosten)
- Alternativ werden Load-Balancing Firewalls verwendet

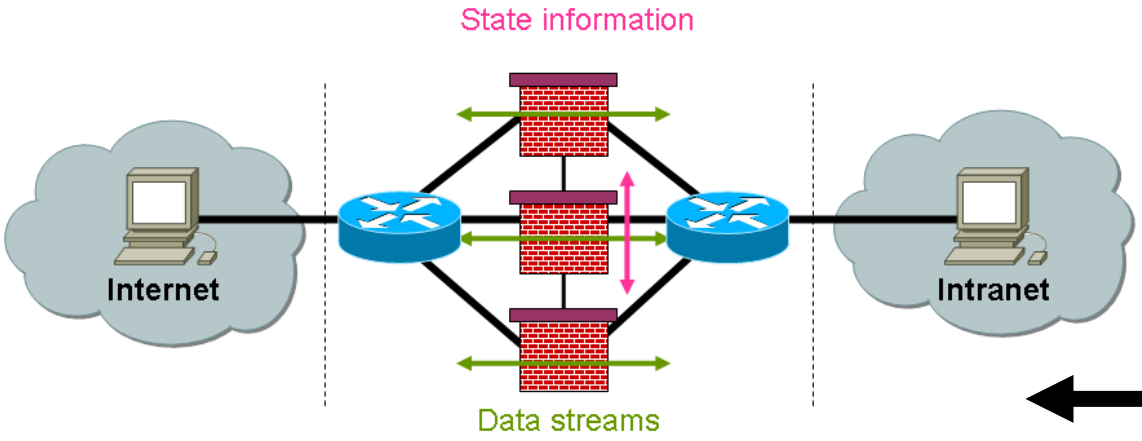
Speziallösungen: Load-Balancing Firewalls

- Heutige Firewall-Systeme bieten maximale Transferrate 1 bis 10 Gbit/s
- Bei höherem Bedarf: Firewall-Verbund
  - je nach Hersteller Firewall-Cluster, Load-Balancing Firewall oder Firewall-Farm
- Verbünde arbeiten meist nach dem Master-Slave-Prinzip
- Master-Firewall verteilt den Verkehr auf die Slave-Firewalls
- Unterschiede bestehen im Wesentlichen im Verteil-Algorithmus
  - Verteilung der Kommunikationsströme
  - Round Robin Paket Verteilung
  - Verteilung durch vorgelagerte Instanz (meist Switch oder Router)
- Realisierung entscheidet über Geschwindigkeit und Nutzen
  - Austausch von Zustandsinformationen
  - Ein Kommunikationsstrom auf einen Slave begrenzt
  - Aufteilung nach Adressen

Speziallösungen: Load-Balancing Firewalls im Bild

Load-Balancing
durch Routing





Load-Balancing
durch Round Robbin

Speziallösungen: Dyna-Fire und CODO

- Dyna-Fire
  - Software-Erweiterung für Netfilter-Iptables
  - Änderung von Filterregeln durch Anwendungs-Requests
  - Port-Knocking: Anwendung generiert in vorgegebener Form Zugriffe auf gesperrte Ports
  - Firewall öffnet vordefinierte Ports entsprechend zentraler User-Datenbank und Ressource Informationen

- Cooperative On-Demand Opening (CODO)
  - Erweiterung für Netfilter-Iptables
  - Firewall stellt 3 offene Ports für Requests zur Verfügung:
    - *Port 1: Server signalisieren Kommunikationsbereitschaft*
    - *Port 2: Externe Anwendungen stellen Öffnungs-Anforderungen*
    - *Port 3: Signalisierung interner Anwendungen für Kommunikationsbedarf nach aussen*
  - Signalisierungskanäle nutzen SSL und X.509 Zertifikate

Speziallösungen: GCB und UDP-Hole-Punching

- Generic Connection Brokering
  - beteiligte Anwendungsprozesse (Client und Server) tauschen über Connection Broker Port-Informationen aus
  - Connection Broker kann als Gateway genutzt werden
  - Linken der Anwendungen mit einer entsprechenden GCB-Bibliothek notwendig

- UDP Hole Punching
  - nutzt Mechanismus eines Intermediate-Gateway
  - Folge von UDP Paketen mit gleichem Quadrupel (Source-IP, Source-Port, Dest-IP, Dest-Port) als UDP-Ströme
  - Informationsaustausch des Quadrupels über einen Server
  - Server steht in sicherer Umgebung, z.B. DMZ
  - Nutzung des Verhaltens erlaubt Kommunikation zweier unabhängige Prozesse über Firewall hinweg
  - UDP-basierter File-Transfer, z.B. UDT, möglich
  - Als Funktionstest in einer Bachelor-Arbeit in UNICORE integriert

Speziallösungen: ALG, Proxies und TBF

- Application Level Gateway und Proxies
  - Anwendungs-Gateway seit Mitte der 90iger bekannt (TIS-Toolkit)
  - Häufig Serverseitig verschiedene oft veraltete Versionen
  - Gateway erlaubt an einer Stelle aktuellen Server-Code, der mit externen Clients kommuniziert
  - Neue Verbindung vom Gateway nach innen
  - Einfachstes Beispiel: FTP-Gateway
    - Client überträgt Datei zum Gateway
    - Datei wird zwischengespeichert und
    - in neuer Verbindung an das Ziel weitergegeben

- Token Based Firewalling in Hybrid GMPLS networks (Policy based Access Control)
  - Signalisierung von Hochgeschwindigkeitsdatenströmen, und damit das sichere Rerouting über alternative schnelle Pfade, wird von heutigen Firewalls noch nicht adressiert
  - Ansatz für mögliches Signalisierungskonzept stellt TBF dar.

Offene Probleme

Existierende Lösungen decken nicht alle Probleme ab

- Anwendungen, die ein oder mehrere dynamische im Vorfeld nicht bekannte Ports/Verbindungen zur Laufzeit des Programms öffnen
- bei Grid-Anwendungen häufig Client-Server-Verbindungen, die Kommunikations-Ports erst vor tatsächlicher Nutzung durch Betriebssystem mitgeteilt bekommen

- Vorheriger Antrag beim Firewall-Administrator nicht möglich
- Wenn Server-Ports vordefiniert, dann sind diese Ports über langen Zeitraum geöffnet

- Was fehlt ist eine allgemeine Lösung, die
  - derartige Problemstellungen adressiert,
  - einfach zu implementieren und durchsatzstark ist,
  - für jede beliebige Art von Ports nutzbar ist,
  - den allgemein üblichen Sicherheits-Richtlinien entspricht und
  - „last-but-not-least“ einem wohldefinierten Standard folgt.

Speziallösungen: DGI2 FG3.3

Im DGI1 Analyse bestehender Ansätze für dynamische Konfiguration von Firewalls durch In-Band oder Out-of-Band Signalisierung untersucht

Von keinem dieser Ansätze in wenigen Jahren eine allgemein akzeptierte und tatsächlich breit einsetzbare Lösung zu erwarten

Firewalls für dynamische Protokolle analysieren den Verkehr der Kontrollverbindungen, um die benötigten Freischaltungen zu erkennen.

Für eine kurzfristig im D-Grid einsetzbare Lösung soll ein geeignetes bekanntes Protokoll ausgewählt und emuliert werden, welche den Firewalls die benötigten dynamischen Freischaltungen signalisiert.

Ziel: Dynamische Konfiguration

- Prototypische Implementierung einer Bibliothek
- zur Einbindung in bestehende Grid-Anwendungen
- transparent für Anwender
- autorisierte, dynamische Öffnung von Ports für die Anwendung
- Lösung mit heute eingesetzten Firewall-Systemen kompatibel
- keine administrativen Eingriffe erforderlich

Speziallösungen: DGI2 FG3.3 (2)

Aufgaben im Bereich der dynamischen Konfiguration (Meilensteine)

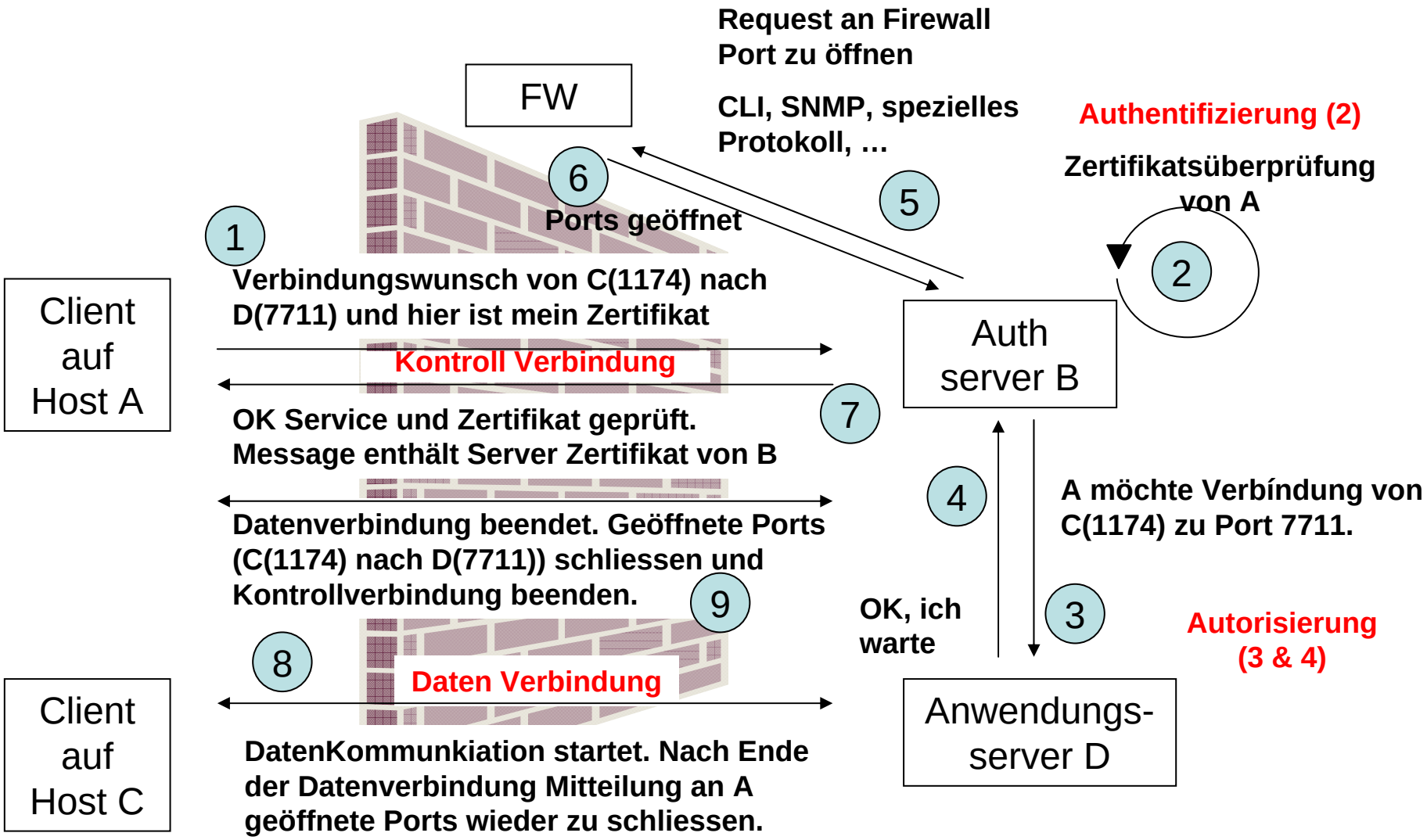
- Aktualisierung, Analyse und Bewertung der durch aktuelle Firewalls inspizierbaren Kommunikationsprotokolle
- Erstellen einer prototypischen Software-Bibliothek für die dynamische Freischaltung von Firewall-Ports
- Bibliothek ist in eine relevante Grid-Anwendungen zu integrieren
- Bibliothek und Anwendung in Produktionsumgebung evaluiert und optimiert
- Communities beim Einsatz beraten

Stand:

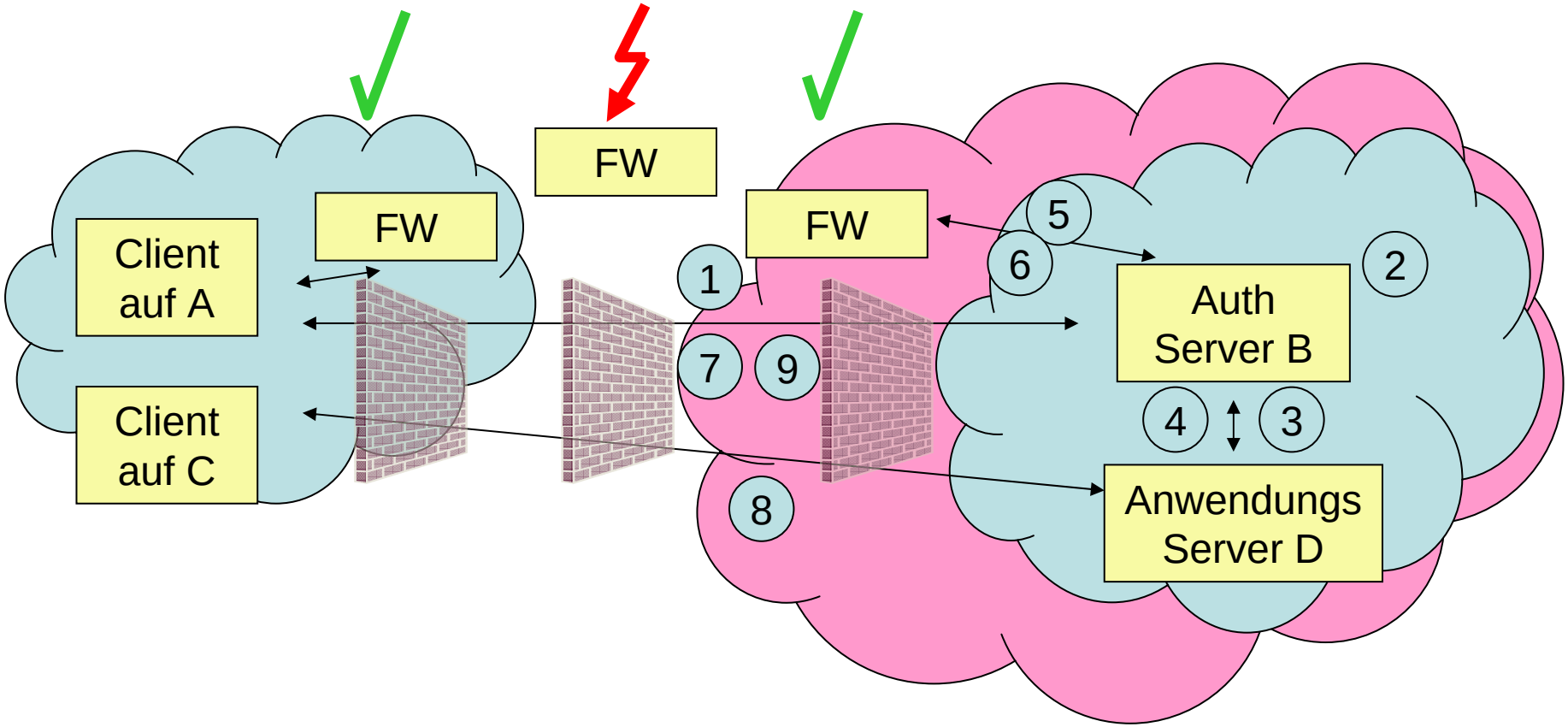
- Auswahl des Kommunikationsprotokolls: FTP
- Prototypische Software-Bibliothek wird derzeit erstellt

Dynamische Konfiguration von Firewalls

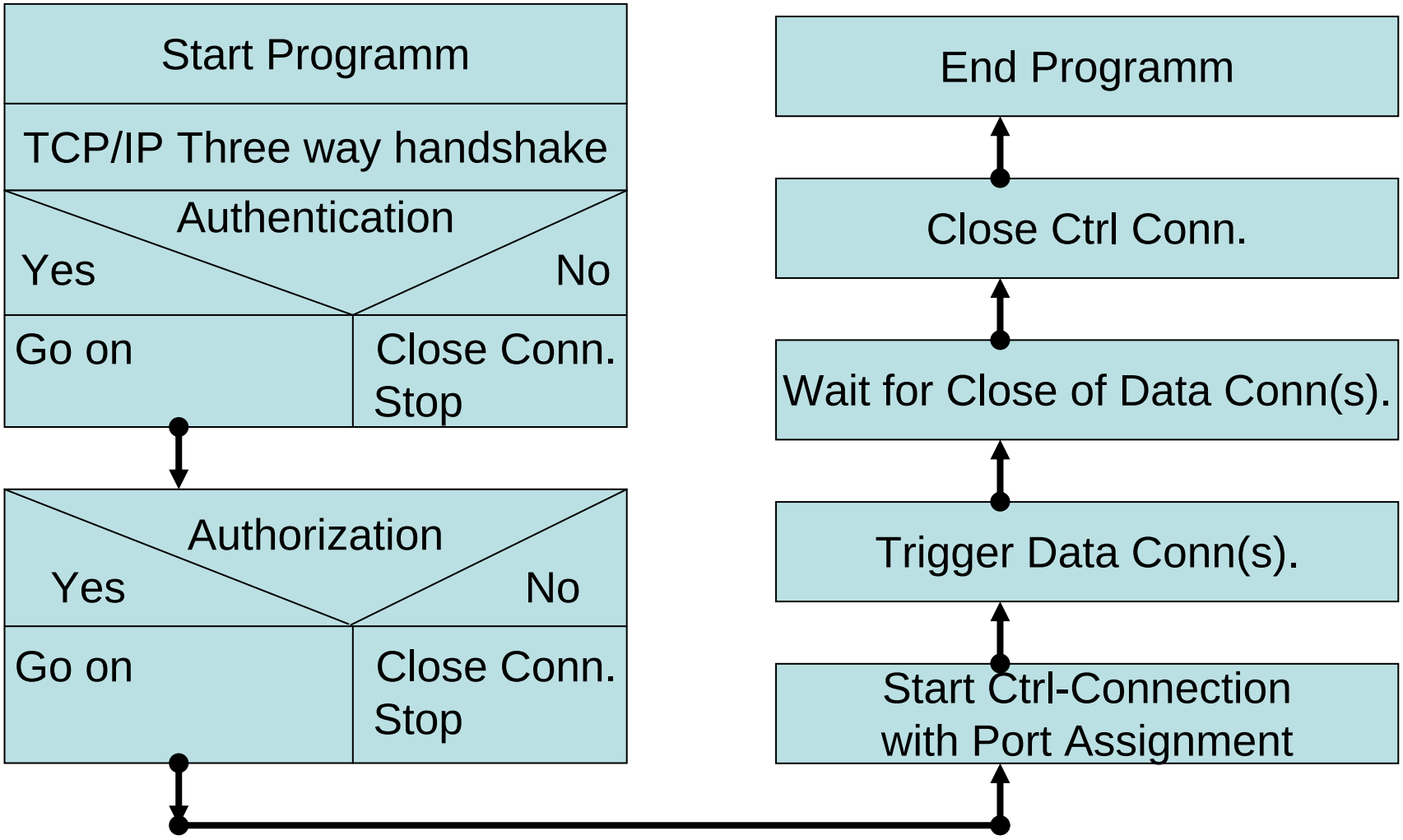
FW opening – Design Prinzip



Dynamische FW Öffnung
Mehrere lokale, entfernte und externe FWs



Program flow chart



Vom File Transfer Protokoll zum Firewall Traversal Protokoll (1)

FTP Protokoll wird von den meisten Firewalls erkannt

FTP nutzt zwei Verbindungen

- Kontroll- und Daten-Verbindung

FTP hat allerdings einige Nachteile:

- Authentifizierung erfolgt im Klartext
- RFC959 erlaubt im Prinzip mehrere parallele Datenverbindungen. Wird aber derzeit von den wenigsten FWs unterstützt. Meist nur eine parallel

Grid-Anwendungen benötigen mehrere für hohen Durchsatz

Oft nutzen Grid-Anwendungen auch “n” ad-hoc parallele Verbindungen (z.B. n Rechenknoten, Datenserver, …)

Vom FTP zum FiTP (2)

Überprüfung des RFC 959 “File Transfer Protocol” führt zu einfacher Lösung:

- Lösche alles, was nicht notwendig ist
- Ändere Dinge, die uns nicht gefallen
- Ergänze das, was wir zusätzlich brauchen
- Berücksichtige immer die Sicherheit

Ergebnis ist ein neues Protokoll, das einfach und leicht zu implementieren ist und häufig genutzt wird

Zu beachten ist:

FiTP kann nur zur Signalisierung von Datenverbindungen genutzt werden, die den gleichen Pfad wie die Kontrollverbindung nutzen

Vom FTP zum FiTP (3)

FiTP wird nicht direkt nach der Standardisierung in Firewall Systemen zur Verfügung stehen

Eine Zwischenlösung muss entwickelt werden

Installation einer Routine Serverseitig zur Signalisierung der zu öffnenden Ports durch CLI oder Spezial-Software

AddOn:

Signalisierungsroutine kann genutzt werden, um Firewalls, die nicht auf dem Pfad der Kontrollverbindung liegen zu konfigurieren

Vom FTP zum FiTP (4)

Anforderungen:

- Nachrichten Integrität
- Schlüsselaustausch (verschlüsselt)
- Authentisierung und Autorisierung (verschlüsselt)
- Kontrollinformation (Klartext)
- Bestätigungen (Klartext)
- Datenverbindung (Out of Scope)
- Ende der Kontrollverbindung (Klartext)

SSH bietet vieles davon, allerdings ist auch die Kontrollinformation verschlüsselt

SSH None Cipher Switching im Überblick

HPN SSH/SCP NONE Cipher Switching

by Chris Rapier PSC, Michael Stevens CMU,
email: hpn-ssh@psc.edu

Volle Verschlüsselung für Schlüsselaustausch, Authentifizierung und Autorisierung

Bei NONE cipher werden die Daten mittels des SSH Protokolls ohne Verschlüsselung übertragen

Minimiert die CPU-Last

Erhöht Durchsatz drastisch

Verschlüsselung für viele Binärdaten nicht notwendig

Zur Sicherstellung der Datenintegrität (man in the middle attacks) wird Hashed Message Authentication Code (HMAC) weiter verwendet

FiTP & SSH-NONE Cipher Relationship

FiTP benutzt eine Modifikation des SSH Protokolls auf der Kontrollverbindung

Zur Implementierung gibt es mehrere Möglichkeiten:

- SSH NONE Cipher als Wrapperprogramm
- Implementierung als Software Library

Die derzeit angedachte Lösung:

- Implementierung als Software Library mit
- Schlüsselaustausch, Authentifizierung und Autorisierung, sowie Grant Access Requests als Unterprogrammaufrufen

Erlaubt einfache Einbindung in Anwendungsprogramme

Kommando Syntax

Kommandos sind Textstrings beginnend mit 4-stelligem Code gefolgt von lesbarem Text und Argument-Felder.

Groß/Kleinschreibung identisch

Beispiel (alle gleich):

3000,GAcR,ACK,Allow=*00020,TCP*,123.045.067.089/32*,12345,12359,124.111.222.233/32,05000,05010*

3000,gacr,ack,allow=*00020,tcp*,123.045.067.089/32*,12345,12359,124.111.222.233/32,05000,05010*

3000,GACR,ACK,ALLOW=*00020,TCP*,123.045.067.089/32*,12345,12359,124.111.222.233/32,05000,05010*

3000,Gacr,Ack,Allow=*00020,Tcp*,123.045.067.089/32*,12345,12359,124.111.222.233/32,05000,05010*

Sicherheitsbetrachtungen (1)

FiTP erlaubt einfache dynamische Konfiguration von FW durch autorisierte Personen

Sicherheitsvergleich mit IPSEC.

- Sicherheit wird durch Überprüfung auf Serverseite gewährleistet
- Wenn empfangende Seite Packet Forwarding erlaubt, können Tunnel etabliert werden

Gleiches Prinzip gilt für FiTP:

- Kontroll-Verbindung via Firewall zu internen Servern erlaubt
- Durch dynamische Anforderungen externer berechtigter Personen werden Verbindungen zu internen Rechnern freigeschaltet
- Auch hier überprüft interner Server die Berechtigung

Haupt-Unterschied:

Mit FiTP weiss man, wer mit wem kommuniziert

Sicherheitsbetrachtungen (2)

- FiTP nutzt allgemein gebräuchliche Techniken für sichere Kommunikation
- Es benutzt das bekannte SSH Protokoll zur Übertragung von FiTP Kommandos
- Verschlüsselung des Authentifizierungs- und Autorisierungs-Prozesses
- Kein man-in-the-middle kann Nachrichten einschleusen oder verändern (Schutz durch HMAC)
- Nachrichten können von der Gegenseite auf Veränderungen überprüft werden
- Bei jeglicher Anomalie können beide Seiten die Kontroll-Verbindung abbrechen

- Strikte Implementierung der Firewall-Regel:
  - Wenn irgend etwas falsch läuft, soll kein Zugriff erlaubt sein.

Stand der Arbeiten zum FiTP

- Draft Protokoll Beschreibung in der OGF Arbeitsgruppe vorgestellt
- Derzeit Verbreitung der Beschreibung zwecks Diskussion und Weiterentwicklung

Dann parallel:

- Kontaktaufnahme mit IETF zwecks Standardisierung
- Implementierung eines ersten sehr limitierten Prototypen
  - Prototyp-Implementierung für Linux-Iptables
  - Prototyp zusammen mit einem Firewall-Hersteller
  - Prototyp für“out of band signalling“
    - *Autorisierungsserver nutzt CLI, spezielle FW-Management Software, HTTPS, …*

Zusammenfassung und Ausblick

Eine Sicherheitskriterien berücksichtigende dynamische Freischaltung von Firewall-Systemen entscheidend für erfolgreiches Arbeiten in VOs.

Nur Konzentration auf einen gemeinsam genutzten Standard für Grid-Anwendungen kann Entwicklungen bei Firewall-Herstellern bewirken.

Dies ist das Ziel der derzeitigen Bemühungen sowohl im D-Grid als auch in internationalen Wissenschafts-Communities wie dem Open Grid Forum und der IETF.

Dieser Vortrag sollte einen Überblick über den Status dieser Arbeiten geben, soll aber andererseits auch zur Mitarbeit an solchen Forschungsaktivitäten anregen.

Nur ein von einer großen Community getragener und auf diese zugeschnittener Standard kann diese Ziele Wirklichkeit werden lassen.

Referenzen

D-Grid Integrationsprojekt 1 Fachgebiet Sicherheit, Diverse Publikationen, http://dgi.d-grid.de/index.php?id=237

D-Grid Integrationsprojekt 2 Fachgebiet 3.3 „Sicherheit – Firewalls“ Arbeitspunkt 2 „Dynamische Konfiguration“, http://www.dgrid.de/index.php?id=439

OGF Work Group: Firewall Issues – Research Group, https://forge.gridforum.org/sf/docman/do/listDocuments/projects.fi-rg/docman.root

http://www.ogf.org/documents/GFD.83.pdf

http://www.ogf.org/documents/GFD.142.pdf

OGF Work Group: Firewall Virtualization for Grid Applications, https://forge.gridforum.org/sf/docman/do/listDocuments/projects.fvga-wg/docman.root

Mitglied der Helmholtz-Gemeinschaft

JÜLICH
FORSCHUNGSZENTRUM

Fragen und Diskussion