



Fachgebiet 3-5 – Entwicklung und Einsatz von
Firewallkonzepten in Grid-Umgebungen

Empfehlungen zur statischen Konfiguration von Firewalls im D-Grid

Autoren

Gian Luca Volpato (RRZN, Universität Hannover)

Christian Grimm (RRZN, Universität Hannover)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01AK800B gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Index

1	EINFÜHRUNG	5
2	GLOBUS GT2	5
3	GLOBUS GT4	7
4	UNICORE.....	10
5	LITERATURNACHWEIS.....	11
	ANHANG A: BEGRENZUNG EPHEMERAL PORT RANGE IN GLOBUS GT2	12
	ANHANG B: BEGRENZUNG EPHEMERAL PORT RANGE IN GLOBUS GT4	14
	ANHANG C.....	15

Abkürzungsverzeichnis

DMZ	DeMilitarized Zone
GIIS	Grid Information Index Server
GRAM	Grid Resource Acquisition and Management
GRIS	Grid Resource Information Server
GSI	Grid Security Infrastructure
GT2	Globus Toolkit 2
GT4	Globus Toolkit 4
MDS	Monitoring and Discovery System
NJS	Network Job Supervisor

1 Einführung

Das im Januar 2006 vorgelegte Dokument „Static Firewall Configuration for Grid Middleware“ des DGI FG3-5 listet die Ports und Transportprotokolle auf, die bei der Kommunikation mit Grid-Diensten genutzt werden. Daraus ergeben sich unmittelbar die Anforderungen zur statischen Konfiguration von Firewalls, um eine ungehinderte Kommunikation in Grid-Umgebungen zu ermöglichen.

Das vorliegende Dokument fasst die Ergebnisse zusammen und legt eine Empfehlung für die Verwendung einheitlicher Ports vor, um die Administration von Firewalls für Grid-Umgebungen im D-Grid zu vereinfachen. Die empfohlenen Ports sollten auf den Firewalls dauerhaft freigeschaltet werden, wobei die IP-Adressen bzw. IP-Subnetze der beteiligten Systeme soweit wie möglich zu berücksichtigen sind.

Die Betrachtungen umfassen derzeit folgende Grid Middlewares:

1. Globus Toolkit 2 und 4
2. UNICORE

Eine vollständige Betrachtung für LCG2 bzw. gLite wird zu einem späteren Zeitpunkt ergänzt.

Anmerkung

In einem nächsten Schritt wird dieses Dokument um die notwendige Zusammenstellung von IP-Adressen bzw. IP-Subnetzen der relevanten Grid-Dienste erweitert. Hierfür sind zunächst weiterführende Überlegungen notwendig, welche Grid-Dienste zentral oder dezentral bzw. extern oder ausschließlich intern zur Verfügung gestellt werden können. Erst mit diesen Angaben ist eine vollständige Empfehlung zur statischen Konfiguration von Firewalls möglich, die den Schutz und das resultierende Sicherheits-Niveau in Grid-Umgebungen optimiert. Es ist beabsichtigt, die hierfür erforderlichen Arbeiten in Absprache mit den Communities und dem Kern-D-Grid in dem nächsten Berichtszeitraum durchzuführen.

2 Globus GT2

Für GT2-Umgebungen im D-Grid wird die Nutzung folgender Ports auf Servern und Clients empfohlen:

Server	TCP-Ports	Änderung gegenüber Default
GRAM	2119 Bereich 20000-25000	Nein Ja
MDS	2135	Nein
GridFTP	2811 Bereich 20000-25000	Nein Ja
GSI-SSH	2222	Ja
MyProxy	7512	Nein

Client	TCP-Ports	Änderung gegenüber Default
GRAM	Bereich 20000-25000	Ja
GridFTP	Bereich 20000-25000	Ja
GSI-SSH	2222 (für Zugriff auf entfernte Server)	Ja

Werden diese Empfehlungen umgesetzt, ergibt sich die im Anhang C beschriebene Firewall-Konfiguration.

2.1 Server

Einrichtungen, die GT2 im Rahmen von D-Grid anwenden, sollten die folgenden Empfehlungen berücksichtigen:

1. Den *controllable ephemeral port range* auf den Bereich 20000 bis 25000 konfigurieren.
2. Den Port für GSI-SSH Server auf 2222/tcp konfigurieren.
3. MDS so konfigurieren, dass sich alle Site-GRIS nur zu einem Parent Site-GIIS innerhalb desselben Netzes bzw. derselben Firewall-Zone anmelden.

Controllable Ephemeral Port Range

Abschätzungen aus dem praktischen Betrieb mit Globus Toolkit zeigen, dass durchschnittlich 20 Ports pro Benutzer auf einem Server genutzt werden. Daraus folgt, dass für eine geschätzte Anzahl von 250 gleichzeitig aktiven Nutzern ein Port-Intervall von 5000 Ports freigegeben werden sollte.

Die Empfehlung für den Bereich 20000-25000 als Port-Intervall im D-Grid begründet sich im Wesentlichen darin, dass LCG2 bzw. gLite diesen Bereich bereits per Default verwenden. Es wäre nicht zu vertreten, für das Globus Toolkit ein zweites Port-Intervall von weiteren 5000 Ports auf den Firewalls freizugeben. Eine Überschneidung des Port-Intervalls mit anderen Anwendungen stellt aus Sicht der Firewall-Administration kein Problem dar, solange die Dienste auf unterschiedlichen Hosts betrieben und somit über verschiedene IP-Adressen erreicht werden.

Die Umgebungsvariable `GLOBUS_TCP_PORT_RANGE` begrenzt die ephemeral Ports auf ein bestimmtes Intervall. Diese Umgebungsvariable wird als *min,max* Wert angegeben (durch Komma separierte Werte). Die Einstellung dieser Umgebungsvariablen in allen Komponenten des Globus Toolkit 2 wird mit einer dreistufigen Prozedur durchgeführt [Wel05]:

1. Konfiguration für GRAM Gatekeeper und Job-Manager
2. Konfiguration für GridFTP
3. Konfiguration für MDS

Anhang A beschreibt detailliert, wie das Port-Intervall auf den Bereich 20000 bis 25000 eingeschränkt werden kann.

GSI-SSH

Der GSI-SSH Server läuft standardmäßig auf dem Port 22/tcp, der auch für reguläre SSH-Verbindungen genutzt wird. Zur getrennten Berücksichtigung beider Dienste in Firewalls wird der Port 2222/tcp für GSI-SSH empfohlen.

Wenn ein GSI-SSH Server bereits installiert ist, ändern die folgenden drei Operationen den bereits konfigurierten Port auf den empfohlenen Wert 2222/tcp:

1. Folgende Zeile in der Datei `$GLOBUS_LOCATION/etc/ssh/sshd_config` ändern:
`Port=2222`
2. Folgende Zeile in die Datei `/etc/services` einfügen:
`gsisshd 2222/tcp`
3. Den `gsisshd` daemon neu starten.

MDS

Die MDS Architektur besteht aus zwei Bestandteilen: GRIS und GIIS. GRIS melden sich an einem oder mehreren Parent GIIS an.

Wenn alle Site GRIS sich nur zu einem Parent GIIS innerhalb desselben Netzes bzw. derselben Firewall-Zone anmelden, interagiert der MDS-Verkehr nicht mit der Site Firewall. Dieses MDS-Modell vereinfacht die Firewall-Konfiguration erheblich, weil es die Kommunikationen nur zwischen externen Clients und den well-known Ports der Server begrenzt.

2.2 Client

Nutzer, die GT2 im Rahmen von D-Grid anwenden, sollten die folgenden Empfehlungen berücksichtigen:

1. Den *controllable ephemeral port range* auf den Bereich 20000 bis 25000 konfigurieren.
2. Den Port für entfernte GSI-SSH Server auf 2222/tcp konfigurieren.

Controllable Ephemeral Port Range

Die Umgebungsvariable `GLOBUS_TCP_PORT_RANGE` begrenzt die ephemeral Ports auf ein bestimmtes Intervall. Diese Umgebungsvariable wird als *min,max* Wert angegeben (durch Komma separierte Werte):

- Folgende Zeile in die Datei `/etc/profile` einfügen:

```
export GLOBUS_TCP_PORT_RANGE=2000,25000
```

GSI-SSH

Der GSI-SSH Client verbindet sich standardmäßig mit den entfernten Servern über den Port 22/tcp. Die folgende Operation ändert den bereits konfigurierten Port auf den empfohlenen Wert 2222/tcp:

- Folgende zwei Zeilen in die Datei `$GLOBUS_LOCATION/etc/ssh/ssh_config` einfügen:

```
Host Server1 Server2 Server3 ... ServerN
    Port 2222
```

Server1 bis ServerN sind die Hostnames der entfernten GSI-SSH Server.

3 Globus GT4

Für GT4-Umgebungen im D-Grid wird die Nutzung folgender Ports auf Servern und Clients empfohlen:

Server	Port	Änderung gegenüber Default
WS-GRAM	8443	Nein
	Bereich 20000-25000	Ja
WS-MDS	8443	Nein
GridFTP	2811	Nein
	Bereich 20000-25000	Ja
RFT	8443	Nein
GSI-SSH	2222	Ja
MyProxy	7512	Nein
Client	Port	Änderung gegenüber Default
WS-GRAM	Bereich 20000-25000	Ja
	2811	Nein
GridFTP	Bereich 20000-25000	Ja
	2222	Ja
GSI-SSH	(für Zugriff auf entfernte Server)	

Werden diese Empfehlungen umgesetzt, ergibt sich die im Anhang C beschriebene Firewall-Konfiguration.

3.1 Server

Einrichtungen, die GT4 im Rahmen von D-Grid anwenden, sollten die folgenden Empfehlungen erfüllen:

1. Den *controllable ephemeral port range* auf den Bereich 20000 bis 25000 konfigurieren.
2. Den Port für GSI-SSH Server auf 2222/tcp konfigurieren.

Controllable Ephemeral Port Range

Abuschätzungen aus dem praktischen Betrieb mit Globus Toolkit zeigen, dass durchschnittlich 20 Ports pro Benutzer auf einem Server genutzt werden. Daraus folgt, dass für eine geschätzte Anzahl von 250 gleichzeitig aktiven Nutzern ein Port-Intervall von 5000 Ports freigegeben werden sollte.

Die Empfehlung für den Bereich 20000-25000 als Port-Intervall im D-Grid begründet sich im Wesentlichen darin, dass LCG2 bzw. gLite diesen Bereich bereits per Default verwenden. Es wäre nicht zu vertreten, für das Globus Toolkit ein zweites Port-Intervall von weiteren 5000 Ports auf den Firewalls freizugeben. Eine Überschneidung des Port-Intervalls mit anderen Anwendungen stellt aus Sicht der Firewall-Administration kein Problem dar, solange die Dienste auf unterschiedlichen Hosts betrieben und somit über verschiedene IP-Adressen erreicht werden.

Die Umgebungsvariable `GLOBUS_TCP_PORT_RANGE` begrenzt die ephemeral Ports auf ein bestimmtes Intervall. Diese Umgebungsvariable wird als *min,max* Wert angegeben (durch Komma separierte Werte). Die Einstellung dieser Umgebungsvariablen in allen Komponenten des Globus Toolkit 4 wird mit einer zweistufigen Prozedur durchgeführt [Wel05]:

1. Konfiguration für C Bibliotheken, Client-Applikationen und Services
2. Konfiguration für Java Bibliotheken, Client-Applikationen und Services

Anhang B beschreibt detailliert, wie das Port-Intervall auf den Bereich 20000 bis 25000 eingeschränkt werden kann.

GSI-SSH

Der GSI-SSH Server läuft standardmäßig auf dem Port 22/tcp, der auch für reguläre SSH-Verbindungen genutzt wird. Zur getrennten Berücksichtigung beider Dienste in Firewalls wird der Port 2222/tcp für GSI-SSH empfohlen.

Wenn ein GSI-SSH Server bereits installiert ist, ändern die folgenden drei Operationen den bereits konfigurierten Port auf den empfohlenen Wert 2222/tcp:

1. Folgende Zeile in der Datei `$GLOBUS_LOCATION/etc/ssh/sshd_config` ändern:
`Port=2222`
2. Folgende Zeile in die Datei `/etc/services` einfügen:
`gsisshd 2222/tcp`
3. Den `gsisshd` daemon neu starten.

3.2 Client

Nutzer, die GT4 im Rahmen von D-Grid anwenden, sollten die folgenden Empfehlungen berücksichtigen:

1. Den *controllable ephemeral port range* auf den Bereich 20000 bis 25000 konfigurieren.
2. Den Port für entfernte GSI-SSH Server auf 2222/tcp konfigurieren.

Controllable Ephemeral Port Range

Die Umgebungsvariable `GLOBUS_TCP_PORT_RANGE` und die Java System Property `org.globus.tcp.port.range` begrenzen die ephemeral Ports auf ein bestimmtes Intervall. Beide Port-Intervalle werden als *min,max* Wert angegeben (durch Komma separierte Werte).

- Eine Zeile in die Datei `/etc/profile` einfügen:
`export GLOBUS_TCP_PORT_RANGE=20000,25000`

- Eine Zeile in die Datei `~/.globus/cog.properties` einfügen, die Java-Bibliotheken lesen automatisch diesen Wert:
`tcp.port.range=20000,25000`

GSI-SSH

Der GSI-SSH Client verbindet sich standardmäßig mit den entfernten Servern über den Port 22/tcp. Die folgende Operation ändert den bereits konfigurierten Port auf den empfohlenen Wert 2222/tcp:

- Folgende zwei Zeilen in die Datei `$GLOBUS_LOCATION/etc/ssh/ssh_config` einfügen:
`Host Server1 Server2 Server3 ... ServerN`
`Port 2222`
Server1 bis ServerN sind die Hostnames der entfernten GSI-SSH Server.

4 UNICORE

Einrichtungen, die UNICORE im Rahmen von D-Grid anwenden, sollten die folgenden Empfehlungen berücksichtigen:

1. Das Gateway in einer DMZ installieren.
2. Den Port des Gateways auf 4433 einstellen.
3. Den Port des NJS auf 8181 einstellen.
4. Die Kommunikation zwischen Gateway und NJS erlauben.

Das Gateway ist der einzige Kontaktknoten für alle externen und internen UNICORE-Verbindungen und funktioniert wie ein Filter vor dem NJS. Das Gateway sollte in einer DMZ installiert werden und alle seine nicht benötigten Services sollten deinstalliert oder gesperrt werden.

Das Gateway erwartet externe Clientverbindungen und Verbindungen der NJSs standardmäßig auf dem Port 4433/tcp. Dieser Port ist in der Datei *gateway/conf/gateway.properties* durch den Parameter *gw.port* konfiguriert [Ber03].

Einrichtungen können einen oder mehrere NJS installieren. Jeder NJS erwartet Client-Verbindungsanfragen vom Site-Gateway standardmäßig auf dem Port 8181/tcp. Dieser Port ist in der Datei *njs/conf/njs.properties* durch den Parameter *njs.gateway_port* konfiguriert [Ber04].

Die Site Firewall sollte Verbindungen zwischen dem Gateway und den NJSs erlauben.

Werden diese Empfehlungen berücksichtigt, ergibt sich die im Anhang C beschriebene Firewall-Konfiguration.

5 Literaturnachweis

- [Wel05] V.Welch. *Globus Toolkit Firewall Requirements*. Version 7, August 2005
<http://www.globus.org/toolkit/security/firewalls/Globus%20Firewall%20Requirements-7.pdf>
- [Ber03] S.van den Berghe, *Using the UNICORE Gateway 4.0.1*, Version 4.0.1, February 2003
http://unicore.sourceforge.net/docs/gateway_manual.pdf
- [Ber04] S.van den Berghe, *Using the NJS and TSI (V4)*, Version 4.1.0, June 2004
http://unicore.sourceforge.net/docs/njs_tsi_manual.pdf

Anhang A: Begrenzung ephemeral port range in Globus GT2 nach [Wei05]

Konfiguration der GT Bibliotheken

- Eine Zeile in die Datei `/etc/profile` einfügen:
`export GLOBUS_TCP_PORT_RANGE=20000,25000`

Konfiguration GRAM Gatekeeper und Job-Manager

Für die Konfiguration von GRAM Gatekeeper und Job-Manager bieten sich drei alternative Möglichkeiten:

1. Verwendung eines Wrapper Script

(den eigentlichen Path von `$GLOBUS_LOCATION` ersetzen):

```
% mv $GLOBUS_LOCATION/libexec/globus-job-manager \
  $GLOBUS_LOCATION/libexec/globus-job-manager.real
% cat > $GLOBUS_LOCATION/libexec/globus-job-manager
#!/bin/sh
GLOBUS_TCP_PORT_RANGE=20000,25000
export GLOBUS_TCP_PORT_RANGE
exec $GLOBUS_LOCATION/libexec/globus-job-manager.real „$@"
^D
% chmod 755 $GLOBUS_LOCATION/libexec/globus-job-manager
```

2. Verwendung des inet Daemon

Eintrag für den Gatekeeper in der Datei `inetd.conf` ändern

(den eigentlichen Path von `$GLOBUS_LOCATION` ersetzen):

```
gatekeeper stream tcp nowait root \
  /bin/env env GLOBUS_TCP_PORT_RANGE=20000,25000 \
  $GLOBUS_LOCATION/sbin/globus-gatekeeper -conf \
  $GLOBUS_LOCATION/etc/globus-gatekeeper.conf
```

3. Verwendung des xinet Daemon

Eintrag in die Datei `/etc/xinetd.d/globus-gatekeeper` hinzufügen

(den eigentlichen Path von `$GLOBUS_LOCATION` ersetzen):

```
service globus-gatekeeper
{
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    server = $GLOBUS_LOCATION/sbin/globus-gatekeeper
    server_args = -conf $GLOBUS_LOCATION/etc/globus-gatekeeper.conf
    disable = no
    env += GLOBUS_TCP_PORT_RANGE=20000,25000
}
```

Konfiguration GridFTP

Für die Konfiguration von GridFTP bieten sich zwei alternative Möglichkeiten an:

1. Verwendung des inet Daemon

Eintrag für den gsiftp in der Datei *inetd.conf* ändern
(den eigentlichen Path von `$GLOBUS_LOCATION` ersetzen):

```
gsiftp stream tcp nowait root \  
    /bin/env env GLOBUS_TCP_PORT_RANGE=20000,25000 \  
    $GLOBUS_LOCATION/sbin/in.ftpd -l -a
```

2. Verwendung des xinet Daemon

Eintrag in die Datei */etc/xinetd.d/gsiftp* hinzufügen
(den eigentlichen Path von `$GLOBUS_LOCATION` ersetzen):

```
service gsiftp  
{  
    socket_type = stream  
    protocol = tcp  
    wait = no  
    user = root  
    server = $GLOBUS_LOCATION/sbin/in.ftpd  
    server_args = -l -a  
    disable = no  
    env += GLOBUS_TCP_PORT_RANGE=20000,25000  
}
```

Konfiguration MDS

- Eine Zeile in die Datei *\$GLOBUS_LOCATION/sbin/SXXgris* einfügen:
`GLOBUS_TCP_PORT_RANGE=20000,25000`

Anhang B: Begrenzung ephemeral port range in Globus GT4 nach [Wei05]

Konfiguration für C Bibliotheken, Client-Applikationen und Services

Entsprechend zur Konfiguration der GT Bibliotheken gemäß Anhang A.

Konfiguration für Java Bibliotheken, Client-Applikationen und Services:

Die System Property `org.globus.tcp.port.range` begrenzt den ephemeral port range. Es bieten sich drei alternative Möglichkeiten, diesen Wert einzustellen:

1. Eine Zeile in die Datei `~/globus/cog.properties` einfügen, die Java-Bibliotheken lesen automatisch diesen Wert:
`tcp.port.range=20000,25000`
Diese Möglichkeit sollte bevorzugt genutzt werden.
2. Der Wert wird über die Kommandozeile übergeben:
`% java -Dorg.globus.tcp.port.range=20000,25000`
3. Der Wert wird direkt in der Applikation angegeben:
`System.setProperty("tcp.port.range", "20000,25000")`

Konfiguration GridFTP

Entsprechend zur Konfiguration von GridFTP gemäß Anhang A.

Anhang C

Diese Tabelle beschreibt die ankommenden/ausgehenden Netzwerkverbindungen für Systeme, die **GT2 Services** nutzen.

Legende CEPR = Controllable Ephemeral Port Range: 20000 bis 25000.

Die Umgebungsvariable GLOBUS_TCP_PORT_RANGE konfiguriert diesen Port Range.

Service	Source		Destination	
	Host	Port (TCP)	Host	Port (TCP)
GRAM Gatekeeper	External clients	*	Localhost	2119
	Localhost	CEPR	External clients	*
GRAM Job-Manager	External clients	*	Localhost	CEPR
	Localhost	CEPR	External clients	*
MDS GRIS	External clients	*	Localhost	2135
MDS GIIS	External clients	*	Localhost	2135
GridFTP control	External clients	*	Localhost	2811
GridFTP data (single channel)	External clients	*	Localhost	CEPR
GridFTP data (multiple channel)	External clients	*	Localhost	CEPR
GridFTP data (multiple channel)	Localhost	CEPR	External clients	*
GSI-SSH	External clients	*	Localhost	2222
MyProxy	External clients	*	Localhost	7512

Wenn alle Einrichtungen, die GT2 im Rahmen von D-Grid verwenden, die vorgeschlagene Empfehlungen umsetzen, werden Wildcards * durch CEPR ersetzt.

Dann findet jede Datenkommunikation immer zwischen einem Port aus einem bestimmten Intervall und einem well-known Port statt oder zwischen Prozessen, die beide Ports aus dem festgelegten Intervall benutzen..

Diese Tabelle beschreibt die ankommenden/ausgehenden Netzwerkverbindungen für Systeme, die **GT4** Services nutzen

Legende CEPR = Controllable Ephemeral Port Range: 20000 bis 25000.

Die Umgebungsvariable GLOBUS_TCP_PORT_RANGE und die Java System Property org.globus.tcp.port.range konfigurieren diesen port range.

Service	Source		Destination	
	Host	Port (TCP)	Host	Port (TCP)
GRAM (job startup and control)	External clients	*	Localhost	8443
	Localhost	CEPR	External clients	*
MDS	External clients	*	Localhost	8443
GridFTP control	External clients	*	Localhost	2811
GridFTP data (single channel)	External clients	*	Localhost	CEPR
GridFTP data (multiple channel)	External clients	*	Localhost	CEPR
GridFTP data (multiple channel)	Localhost	CEPR	External clients	*
GSI-SSH	External clients	*	Localhost	2222
MyProxy	External clients	*	Localhost	7512

Wenn alle Einrichtungen, die GT2 im Rahmen von D-Grid verwenden, die vorgeschlagene Empfehlungen umsetzen, werden Wildcards * durch CEPR ersetzt.

Dann findet jede Datenkommunikation immer zwischen einem Port aus einem bestimmten Intervall und einem well-known Port statt oder zwischen Prozessen, die beide Ports aus dem festgelegten Intervall benutzen.

Diese Tabelle beschreibt die ankommenden/ausgehenden Netzwerkverbindungen für Systeme, die **UNICORE** Services nutzen.

Service	Source		Destination	
	Host	Port (TCP)	Host	Port (TCP)
Gateway (in der DMZ)	external hosts	*	Localhost	4433
	Localhost	*	NJS	8181
	NJS	8181	Localhost	*
NJS (in innerem Netzwerk)	Localhost	8181	Gateway	*
	Gateway	*	Localhost	8181