



***GNU GATEKEEPER ALS
INSTELLINGSGATEKEEPER***
*HANDLEIDING VOOR HET CONFIGUREREN
VAN EEN GNU GATEKEEPER ALS GDS
GATEKEEPER*

Versie 1.0, 13 juni 2010

Bert Andree, Ant Arbor

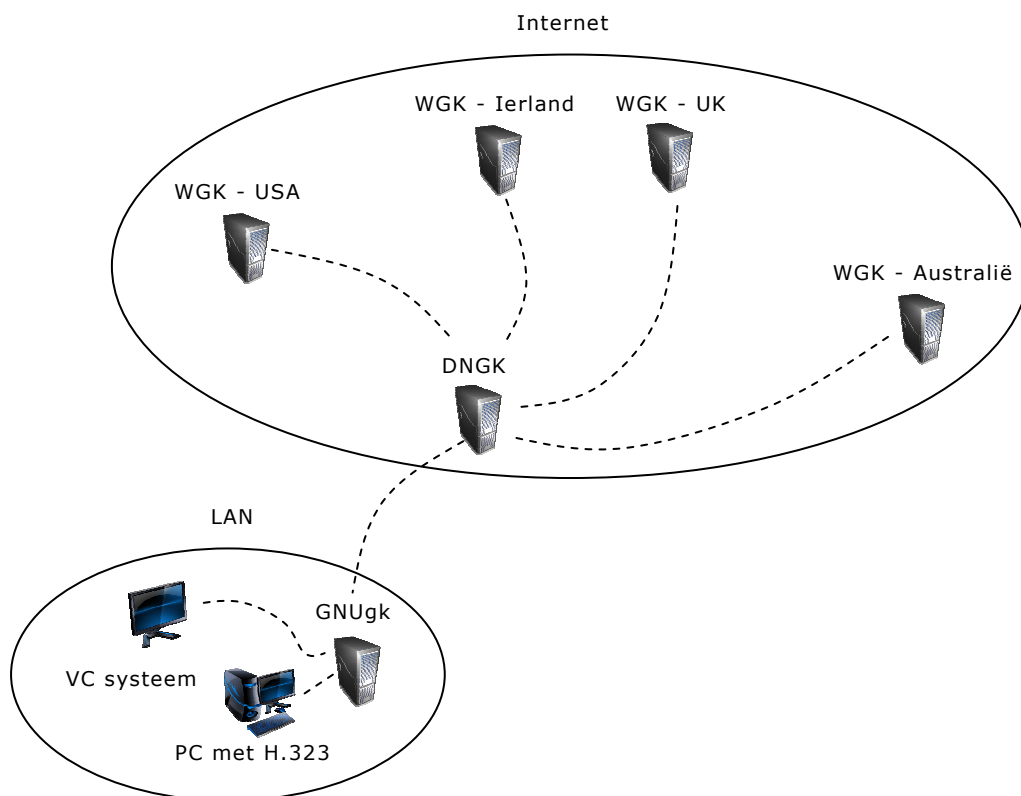
CONTENTS

1	Introductie	3
2	Scenario's.....	4
2.1	Open Internet connectie	4
2.2	Publiek Internet adres met Firewall	4
2.3	Niet routeerbaar IP adres met NAT	4
3	Implementatie	5
3.1	Algemene installatie	5
3.2	Specifieke configuratie per scenario	5
Appendix A.	Installatie en configuratie	10
A.1	Download	10
A.2	Installatie	10
A.3	Firewall voor scenario 1.....	11
A.4	Firewall voor scenario 2 en 3	11
A.5	gatekeeper.ini voor scenario 1	12
A.6	gatekeeper.ini voor scenario 2 en 3.....	13

1 INTRODUCTIE

Dit document beschrijft het opzetten van een GNU Gatekeeper als instellingsgatekeeper en de koppeling hiervan met GDS (zie: http://en.wikipedia.org/wiki/Global_Dialing_Scheme). De opzet zoals deze beschreven is in dit document is van toepassing voor alle instellingen die binnen Nederland een GNU gatekeeper met GDS willen koppelen.

De plaats van de instellingsgatekeeper in de GDS hiërarchie is schematisch weergegeven in Figuur 1. Er zijn vier World gatekeepers, ook wel GDS Global Root Gatekeepers genoemd in Ierland, UK, USA en Australië. Een van deze World gatekeepers is dubbel uitgevoerd. De Nederlandse nationale gatekeeper (in het figuur weergegeven als DNGK) is ook dubbel uitgevoerd. Deze gatekeeper is gekoppeld met de World gatekeepers. Wanneer een instelling binnen Nederland op GDS wil aansluiten is het noodzakelijk (en tevens voldoende) om te koppelen met de Nederlandse Nationale gatekeeper. Videoconferentie apparatuur kan dan op de instellingsgatekeeper aangemeld worden.



Figuur 1 schematisch overzicht van de GDS hiërarchie. DNGK (de Nederlandse Nationale gatekeeper) en WGK – UK (de global root in Groot Brittannië) zijn beiden dubbel uitgevoerd.

De beschreven koppelingen kunnen, en mogen, gemaakt worden door in Nederland gevestigde instellingen die een Nederlands telefoonnummerblok bezitten. Een instelling die op GDS wil aansluiten hoeft geen SURFnet klant te zijn.

2 SCENARIO'S

In dit hoofdstuk beschrijven we drie scenario's waarvoor we een GNU Gatekeeper configuratie gemaakt en getest hebben.

2.1 Open Internet connectie

Met betrekking tot H.323 videoconferentie spreken we van een open Internet connectie wanneer een H.323 systeem een publiek IP adres heeft en alle voor H.323 benodigde inkomende en uitgaande poorten open staan. Welke poorten open moeten staan kan afhangen van de gebruikte apparatuur en de gekozen instellingen. Een H.323 systeem op een open Internet connectie kan verbindingen opzetten met andere H.323 systemen op publiek Internet door IP adressen van deze systemen te "bellen". Ook kan een H.323 systeem op een open Internet connectie op dezelfde manier "gebeld" worden.

De toegevoegde waarde van een Gatekeeper met GDS koppeling in dit scenario zit in de extra mogelijkheid van "nummergebaseerd bellen". Het H.323 systeem kan andere H.323 systemen die op GDS aangesloten zijn "bellen" door een nummer te kiezen, ook wanneer het andere systeem achter een Firewall zit. Ook is het mogelijk om rechtstreeks te verbinden met diensten die een IP adres delen. Hierbij kan gedacht worden aan het rechtstreeks inbellen op virtuele vergaderruimtes van een op GDS aangesloten MCU.

2.2 Publiek Internet adres met Firewall

Wanneer een H.323 systeem een publiek Internet adres heeft dat wel achter de Firewall zit is een van de mogelijkheden om een aantal uitgaande en inkomende TCP en UDP poorten open te zetten. Wanneer het vooraf niet exact bekend is met welke partijen een videoconferentie opgezet gaat worden is het nodig om deze poorten te openen voor verkeer vanaf alle netwerklocaties.

Naast ondersteuning van nummergebaseerd bellen zoals in het eerste scenario kan een instellingsgatekeeper voor dit scenario extra mogelijkheden bieden. Het is mogelijk om de gatekeeper als proxy te laten functioneren. Het configureren van de Firewall wordt dan eenvoudiger en videoconferentie kan vanaf het hele netwerk ondersteund worden zonder alle aanwezige computers extra bloot te stellen aan mogelijke aanvallen van buiten de Firewall.

2.3 Niet routeerbaar IP adres met NAT

Wanneer een H.323 systeem geen publiek Internet adres heeft wordt bellen en gebeld worden erg ingewikkeld. H.323 aware routers maken uitbellen weliswaar mogelijk, maar om gebeld te worden moet poort 1720 doorgezet worden naar het juiste interne adres. Zonder gebruik van gatekeepers is dat alleen mogelijk voor een H.323 systeem.

Voor dit scenario werken we een oplossing uit met een GNU Gatekeeper die zelf een publiek adres heeft. Naast alle eerder genoemde voordelen heeft deze oplossing een mogelijkheid voor NAT Traversal. Dat wil zeggen dat systemen die zelf geen publiek adres hebben via de gatekeeper kunnen bellen en gebeld kunnen worden.

3 IMPLEMENTATIE

3.1 Algemene installatie

3.1.1 Randvoorwaarden en keuzes

We hebben gekozen voor het implementeren van GNUgk op 64 bits RedHat Linux Enterprise Edition 5. Om maximale flexibiliteit te waarborgen maken we gebruik van virtuele machines. Bij de implementatie van GNUgk voor de laatste twee scenario's worden hoge eisen aan de computer gesteld. Of een Virtuele Machine daarvoor krachtig genoeg is hangt van veel factoren af en zal daarom van geval tot geval bekeken moeten worden. Voor het eerste scenario verwachten we geen problemen bij de implementatie van GNUgk op een Virtuele Machine.

We hebben gekozen om uit te gaan van de Linux 64 bit Executable (static, met MySQL, SQLite en H.460.18/.19 support). De keuze voor het gebruik van static binaries is gemaakt om geen afhankelijkheid van libraries te creëren. Een nadeel hiervan is dat specifieke bugs en kwetsbaarheden in binaries meegenomen worden in de GNUgk executable¹ en dus niet automatisch verdwijnen bij het upgraden van de libraries.

Dit document beschrijft het opzetten van een GNU gatekeeper als GDS Gatekeeper. Het GDS nummerplan is gebaseerd op het ITU-T nummerplan voor telefonie. In Nederland nemen we het telefoonnummerplan en de telefoonnummerblokken vrijwel geheel over. Elke instelling kan zich op GDS aansluiten met de eigen gebruikte telefoonnummers. Een uitzondering hierop vormen de 0800 en 0900 nummers. Deze nummers zijn gereserveerd voor diensten. Alle voorbeeldconfiguraties in dit document zijn gemaakt voor een fictieve organisatie met nummerblok 0101234XXX².

3.1.2 Installatie van GNUgk

3.1.2.1 Voorbereiding

Dit document gaat uit van een werkende configuratie van RedHat EL 5, 64 bits. Zorg ervoor dat NTP geïnstalleerd en geconfigureerd is.

3.1.2.2 Download en installatie

Download eerst de GNUgk binaries en pak ze uit. Details hierover zijn te vinden in Appendix A.1. De installatie is beschreven in Appendix A.2.

3.2 Specifieke configuratie per scenario

3.2.1 Open Internet connectie

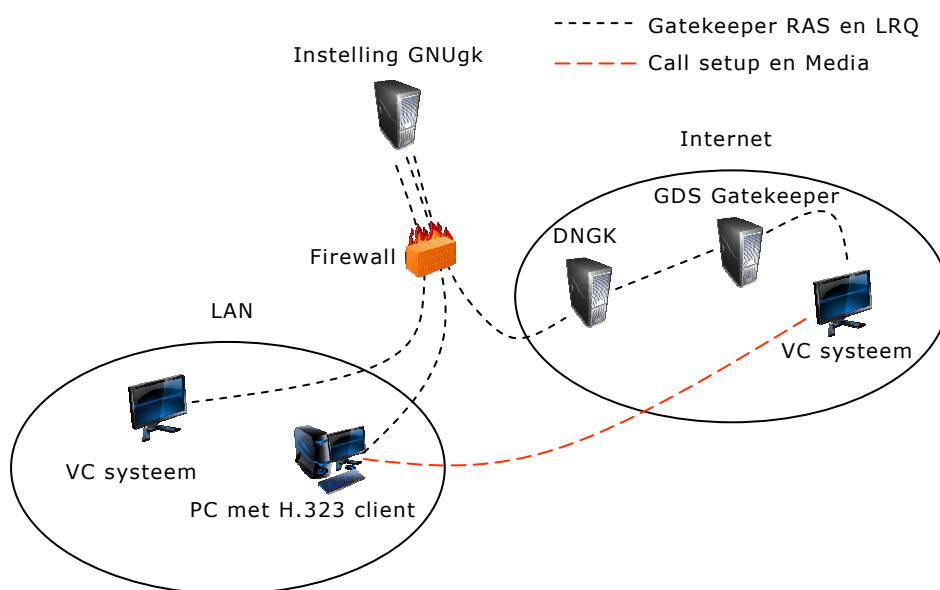
Met betrekking tot H.323 videoconferentie spreken we van een open Internet connectie wanneer een H.323 systeem een publiek IP adres heeft en alle voor H.323 benodigde inkomende en uitgaande poorten open staan. Dit scenario is geïllustreerd in Figuur 2. Een systeem dat gekoppeld is aan een op GDS aangesloten gatekeeper (GDS gatekeeper)

¹ Voor het eerste scenario is dit risico beperkt omdat voor GNU gatekeeper in dat geval alleen UDP poort 1719 opengezet hoeft te worden.

² Het nummerblok 0101234XXX omvat de telefoonnummers 0101234000 tot en met 0101234999.

plaatst een call via deze GDS gatekeeper, de Nederlandse Nationale gatekeeper (DNGK) en de instellingsgatekeeper (Instelling GNUgk). De instellingsgatekeeper zelf kan wel achter een Firewall geplaatst worden. Voor het functioneren van de gatekeeper is in dit scenario alleen UDP poort 1719 nodig.

Wanneer een op GDS aangesloten videoconferentieapparaat op publiek Internet een call op wil zetten naar een videoconferentieapparaat op het lokale Netwerk (LAN) loopt alleen het opzoeken van de adressen via de gatekeepers. De verkeersstromen (media en call control) worden vervolgens rechtstreeks opgezet tussen beide videoconferentieapparaten.



Figuur 2 scenario met open Internet connectie. De gatekeeper kan achter een Firewall geplaatst worden.

3.2.1.1 Configuratie van Iptables (firewall)

In Appendix A.3 geven we een voorbeeld van een mogelijke iptables file. Naast de voor beheer benodigde poorten moet alleen UDP poort 1719 naar de gatekeeper opengezet worden. Toegang tot de voor beheer benodigde poorten kan indien gewenst nog verder beperkt worden tot een aantal vertrouwde IP adressen binnen de eigen organisatie.

3.2.1.2 Configuratie gatekeeper.ini

In Appendix A.5 geven we een voorbeeld van een mogelijke gatekeeper.ini file. Deze file is geoptimaliseerd voor het eerste scenario. Twee systemen kunnen aangemeld worden met hun volledige internationale 13 cijferige telefoonnummer. Een systeem mag zich alleen aanmelden met een vooraf bepaald IP adres en het tweede systeem mag zich aanmelden met ieder willekeurig IP adres.

De bestanden met logging en call detail records worden wekelijks gerouleerd. De actuele status (registraties en calls) kunnen via de status poort vanuit de lokale machine bekeken worden via telnet 127.0.0.1 op TCP poort 7000. Indien een interne Firewall het

verkeer van de locale host blokkeert dient TCP poort 7000 door deze Firewall vanaf localhost doorgelaten te worden.

Deze gatekeeper.ini file is slechts bedoeld als een initiële configuratie. Ze dient verder aangepast te worden aan de lokale situatie.

3.2.2 Publiek Internet adres met Firewall

Wanneer een H.323 systeem een publiek Internet adres heeft dat wel achter de Firewall zit is een van de mogelijkheden om een aantal uitgaande en inkomende TCP en UDP poorten open te zetten. Wanneer het vooraf niet exact bekend is met welke partijen een videoconferentie opgezet gaat worden is het nodig om deze poorten te openen voor verkeer vanaf alle netwerklocaties. In het bijzonder voor videoconferentie vanaf de werkplek kan het onwenselijk zijn om de Firewall open te zetten voor binnenkomende connecties vanuit het hele Internet. In dat geval is het mogelijk om een GNU Gatekeeper als Proxy op te zetten.

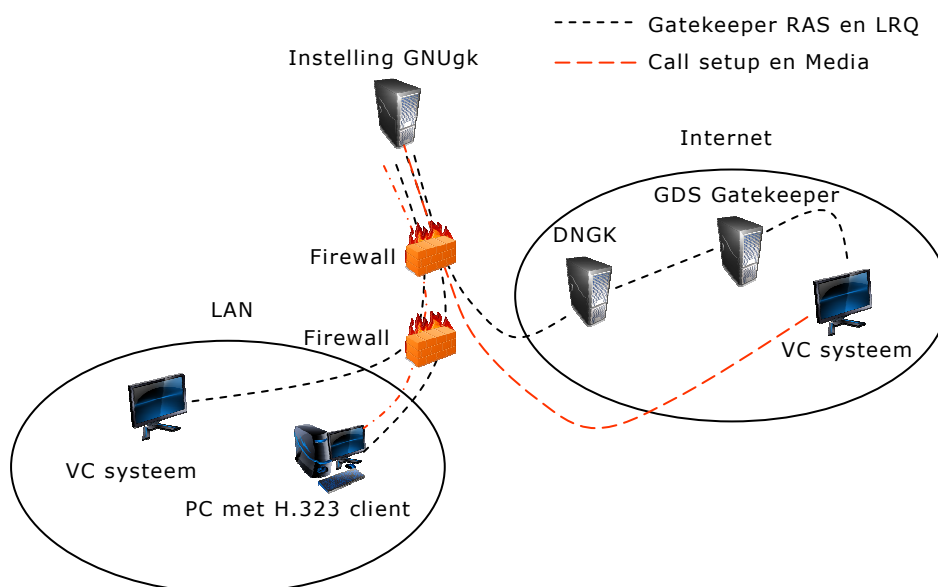
Dit scenario is geïllustreerd in Figuur 3. Een systeem dat gekoppeld is aan een op GDS aangesloten gatekeeper (GDS gatekeeper) plaatst een call via deze GDS gatekeeper, de Nederlandse Nationale gatekeeper (DNGK) en de instellingsgatekeeper (Instelling GNUgk). De instellingsgatekeeper zelf kan achter een DMZ Firewall geplaatst worden. Voor het functioneren van de gatekeeper is in dit scenario een reeks TCP en UDP poorten nodig. Deze poorten worden in Tabel 1 voor de LAN Firewall gegeven.

<i>Source IP</i>	<i>Destination IP</i>	<i>Source Port</i>	<i>Destination Port</i>	<i>Protocol</i>	<i>Beschrijving</i>
LAN	Gatekeeper	1024 - 65535	1719	UDP	Gatekeeper RAS
LAN	Gatekeeper	1024 - 65535	1720	TCP	H.323 Call Signalling
LAN	Gatekeeper	1024 - 65535	30000 - 30999	TCP	Q931PortRange
LAN	Gatekeeper	1024 - 65535	31000 - 31999	UTP	H245PortRange
LAN	Gatekeeper	1024 - 65535	50000 - 50999	TCP	T120PortRange
LAN	Gatekeeper	1024 - 65535	50000 - 50999	UDP	RTPPortRange
Gatekeeper	LAN	1719	1024 - 65535	UDP	Gatekeeper RAS
Gatekeeper	LAN	1720	1024 - 65535	TCP	H.323 Call Signalling
Gatekeeper	LAN	30000 - 30999	1024 - 65535	TCP	Q931PortRange
Gatekeeper	LAN	31000 - 31999	1024 - 65535	UTP	H245PortRange
Gatekeeper	LAN	50000 -	1024 - 65535	TCP	T120PortRange

		50999			
Gatekeeper	LAN	50000 – 50999	1024 – 65535	UDP	RTPPortRange

Tabel 1 overzicht van de voor scenario 2 benodigde open poorten in de DMZ Firewall.

Wanneer een op GDS aangesloten videoconferentieapparaat op publiek Internet een call op wil zetten naar een videoconferentieapparaat op het locale Network (LAN) loopt het opzoeken van de adressen via de gatekeepers. Wanneer het systeem op Internet dat de call opzet zelf niet achter een Firewall zit worden de verkeersstromen (media en call control) van het systeem op Internet via de Instellingsgatekeeper opgezet.



Figuur 3 scenario met videoconferentie achter de Firewall. De gatekeeper kan achter een tweede Firewall geplaatst worden

3.2.2.1 Configuratie van Iptables (firewall)

In Appendix A.4 geven we een voorbeeld van een mogelijke iptables file. Naast de voor beheer benodigde poorten moet alleen UDP poort 1719 naar de gatekeeper opengezet worden. Toegang tot de voor beheer benodigde poorten kan indien gewenst nog verder beperkt worden tot een aantal vertrouwde IP adressen binnen de eigen organisatie.

3.2.2.2 Configuratie gatekeeper.ini

In Appendix A.6 geven we een voorbeeld van een mogelijke gatekeeper.ini file. Deze file is geoptimaliseerd voor het tweede scenario. Twee systemen kunnen aangemeld worden met hun volledige internationale 13 cijferige telefoonnummer. Een systeem mag zich alleen aanmelden met een vooraf bepaald IP adres en het tweede systeem mag zich aanmelden met ieder willekeurig IP adres.

De bestanden met logging en call detail records worden wekelijks gerouleerd. De actuele status (registraties en calls) kunnen via de status poort vanuit de lokale machine bekeken worden via telnet 127.0.0.1 op poort 7000.

Deze gatekeeper.ini file is slechts bedoeld als een initiële configuratie. Ze dient verder aangepast te worden aan de lokale situatie. Enkele oudere systemen kunnen niet goed omgaan met de H.460 berichten. In dat geval kan de regel "EnableH46018=1" gewijzigd worden in "EnableH46018=0".

3.2.3 Niet routeerbaar IP adres met NAT

Wanneer een H.323 systeem geen publiek Internet adres heeft, of wanneer het niet mogelijk of wenselijk is om inkomende verbindingen toe te staan kan de GNU gatekeeper in H.460.18 mode gezet worden. Vanuit het LAN wordt het verkeer via uitgaande verbindingen naar de gatekeeper getunneld.

Dit scenario is vrijwel gelijk aan het tweede scenario. Het verschil zit in de firewall configuratie en in het laten vallen van de eis dat de videoconferentieapparaten over publieke IP adressen beschikken. Voor het functioneren van de gatekeeper is in dit scenario een reeks TCP en UDP poorten nodig. Deze poorten worden in Tabel 2 voor de LAN Firewall gegeven.

<i>Source IP</i>	<i>Destination IP</i>	<i>Source Port</i>	<i>Destination Port</i>	<i>Protocol</i>	<i>Beschrijving</i>
LAN	Gatekeeper	1024 – 65535	1719	UDP	Gatekeeper RAS
LAN	Gatekeeper	1024 – 65535	1720	TCP	H.323 Call Signalling
LAN	Gatekeeper	1024 – 65535	30000 - 30999	TCP	Q931PortRange
LAN	Gatekeeper	1024 – 65535	31000 - 31999	UTP	H245PortRange
LAN	Gatekeeper	1024 – 65535	50000 - 50999	TCP	T120PortRange
LAN	Gatekeeper	1024 – 65535	50000 - 50999	UDP	RTPPortRange

Tabel 2 overzicht van de voor scenario 2 benodigde open poorten in de DMZ Firewall.

Wanneer een op GDS aangesloten videoconferentieapparaat op publiek Internet een call op wil zetten naar een videoconferentieapparaat op het locale Netwerk (LAN) loopt het opzoeken van de adressen via de gatekeepers. Wanneer het systeem op Internet dat de call opzet zelf niet achter een Firewall zit worden de verkeersstromen (media en call control) van het systeem op Internet via de Instellingsgatekeeper opgezet.

3.2.3.1 Configuratie van Iptables (firewall)

De configuratie van de iptables file is identiek aan die van het tweede scenario. Details hierover kunnen gevonden worden in paragraaf 3.2.2.1.

3.2.3.2 Configuratie gatekeeper.ini

De configuratie van de gatekeeper.ini file is identiek aan die van het tweede scenario. Details hierover kunnen gevonden worden in paragraaf 3.2.2.2. Uiteraard mag de regel "EnableH46018=1" voor het derde scenario niet gewijzigd of verwijderd worden.

APPENDIX A. INSTALLATIE EN CONFIGURATIE

A.1 Download

```
[root@surfnetgate ~]# wget
http://prdownloads.sourceforge.net/openh323gk/gnugk-2.3.1-linux-
x86_64.tar.gz?download
[root@surfnetgate ~]# gunzip -c gnugk-2.3.1-linux-x86_64.tar.gz | tar xf -
[root@surfnetgate ~]#
```

A.2 Installatie

```
[root@surfnetgate init.d]# cd /etc/init.d
[root@surfnetgate init.d]# cp /root/gnugk-2.3.1-linux-
x86_64/gk.initd.redhat gnugk
[root@surfnetgate init.d]# chmod +x gnugk
[root@surfnetgate init.d]# cp /root/gnugk-2.3.1-linux-x86_64/bin/gnugk
/usr/sbin/gnugk
[root@surfnetgate init.d]# mkdir /var/log/gk
[root@surfnetgate init.d]# cd /etc/
[root@surfnetgate etc]# cp /root/gnugk-2.3.1-linux-x86_64/etc/gnugk.ini
gatekeeper.ini
[root@surfnetgate etc]#
```

Standaard is de logging van GNU Gatekeeper erg summier. We adviseren om in /etc/init.d/gnugk de volgende wijziging door te voeren.

zoek: \$GKEXE -c \$GKCONFIG -o \$LOGFILE > /dev/null 2>&1 &

en vervang dit door: \$GKEXE -c \$GKCONFIG -o \$LOGFILE -tt > /dev/null 2>&1 &

Laat gnugk automatisch starten:

```
[root@surfnetgate etc]# chkconfig --add gnugk
[root@surfnetgate etc]# chkconfig --list gnugk
gnugk          0:off  1:off  2:off  3:on   4:on   5:on   6:off
[root@surfnetgate etc]#
```

Start gnugk nu via het init.d script.....

```
[root@surfnetgate etc]# /etc/init.d/gnugk start
Starting gnugk:                                     [ OK ]
[root@surfnetgate etc]# /etc/init.d/gnugk status
gnugk (pid 18878) is running...
[root@surfnetgate etc]#
```

A.3 Firewall voor scenario 1

Hieronder staat de iptables file zoals die gebruikt is voor het eerste scenario. Alleen de regel met UDP poort 1719 is in ons geval toegevoegd aan de initiële iptables file.

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 1719 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

A.4 Firewall voor scenario 2 en 3

Hieronder staat de iptables file zoals die gebruikt is voor het tweede en derde scenario.

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 1719 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 1720 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 1503 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 30000:30999 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 31000:31999 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 50000:50999 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 50000:50999 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibitedCOMMIT
```

A.5 gatekeeper.ini voor scenario 1

Hieronder staat de gatekeeper.ini file zoals die gebruikt is voor het eerste scenario.

```
[Gatekeeper::Main]
FortyTwo=42
Name=Scenario1
EndpointSuffix=_Scenario1
TimeToLive=60
; change this to 1 or 2, if you want CDRs and RAS messages to be printed on
the status port
StatusTraceLevel=0
; enable these options if your endpoints use broadcast and/or multicast to
discover the gatekeeper
UseBroadcastListener=0
UseMulticastListener=0

; restrict access to the status port by an IP address
[GkStatus::Auth]
rule=explicit
127.0.0.1=allow
default=forbid

[LogFile]
Rotate=Weekly
RotateDay=Sun
RotateTime=00:59

[Gatekeeper::Acct]
FileAcct=required

[FileAcct]
DetailFile=/var/log/gk/cdr.log
; 1 to use status interface compatible CDRs, 0 to build CDR from CDRString
StandardCDRFormat=1
; parametrized CDR format string
CDRString=%s|%u|{%Calling-Station-Id}|{%Called-Station-Id}|%d|%c
; timestamp format for CDR strings
TimestampFormat=ISO8601
Rotate=weekly
RotateDay=Sun
RotateTime=00:59

[RoutedMode]
; enable gatekeeper signaling routed mode, route H.245 channel only if
necessary (for NATed endpoints)
GKRouted=0

[RoutingPolicy]
default=explicit,internal,parent,neighbor,dns,srv

; proxy calls only for NATed endpoints
[Proxy]
Enable=0

[RasSrv::RRQFeatures]
; endpoint identifiers are assigned by the gatekeeper
AcceptEndpointIdentifier=0
; you may want to disable this, if you want to control gateway prefixes
from the config
AcceptGatewayPrefixes=1
```

```
[CallTable]
; don't print CDRs for neighbor calls to the status port
GenerateNBCDR=1
; print CDRs for unconnected calls to the status port
GenerateUCCDR=1

[RasSrv::LRQFeatures]
AcceptNonNeighborLCF=1
AcceptNonNeighborLRQ=1

[RasSrv::RewriteE164]
0101234.=0031101234.

[RasSrv::Neighbors]
dngk1=GnuGK
dngk2=GnuGK

[Neighbor::dngk1]
GatekeeperIdentifier=DutchNational
Host=dngk1.surfnet.nl
SendPrefixes=0
AcceptPrefixes=*
ForwardResponse=1
ForwardLRQ=always

[Neighbor::dngk2]
GatekeeperIdentifier=DutchNational
Host=dngk2.surfnet.nl
SendPrefixes=0
AcceptPrefixes=*
ForwardResponse=1
ForwardLRQ=always

[Gatekeeper::Auth]
AliasAuth=required;RRQ
default=allow

[RasSrv::RRQAuth]
; Voorgedefinieerde Accounts

; kamer1@scenario1.nl          ;      0031101234100
; wijzig het IP adres in het
; publieke IP adres van het videoconferentieapparaat
0031101234100=sigip:10.10.10.50:1720

; gebruiker1@scenario1.nl     ;      0031101234200
; gebruiker1 mag vanuit alle IP adressen registreren
0031101234200=allow
```

A.6 gatekeeper.ini voor scenario 2 en 3

Hieronder staat de gatekeeper.ini file zoals die gebruikt is voor het tweede en derde scenario.

```
[Gatekeeper::Main]
FortyTwo=42
Name=Scenario1
EndpointSuffix=_Scenario1
TimeToLive=60
```

```
; change this to 1 or 2, if you want CDRs and RAS messages to be printed on
the status port
StatusTraceLevel=0
; enable these options if your endpoints use broadcast and/or multicast to
discover the gatekeeper
UseBroadcastListener=0
UseMulticastListener=0

; restrict access to the status port by an IP address
[GkStatus::Auth]
rule=explicit
127.0.0.1=allow
default=forbid

[LogFile]
Rotate=Weekly
RotateDay=Sun
RotateTime=00:59

[Gatekeeper::Acct]
FileAcct=required

[FileAcct]
DetailFile=/var/log/gk/cdr.log
; 1 to use status interface compatible CDRs, 0 to build CDR from CDRString
StandardCDRFormat=1
; parametrized CDR format string
CDRString=%s|%u|{%Calling-Station-Id}|{%Called-Station-Id}|%d|%c
; timestamp format for CDR strings
TimestampFormat=ISO8601
Rotate=weekly
RotateDay=Sun
RotateTime=00:59

[RoutedMode]
; enable gatekeeper signaling routed mode, route H.245 channel only if
necessary (for NATed endpoints)
GKRouted=0

[RoutingPolicy]
default=explicit,internal,parent,neighbor,dns,srv

; proxy calls only for NATed endpoints
[Proxy]
Enable=0

[RasSrv::RRQFeatures]
; endpoint identifiers are assigned by the gatekeeper
AcceptEndpointIdentifier=0
; you may want to disable this, if you want to control gateway prefixes
from the config
AcceptGatewayPrefixes=1

[CallTable]
; don't print CDRs for neighbor calls to the status port
GenerateNBCDR=1
; print CDRs for unconnected calls to the status port
GenerateUCCDR=1

[RasSrv::LRQFeatures]
AcceptNonNeighborLCF=1
```

```
AcceptNonNeighborLRQ=1
```

```
[RasSrv::RewriteE164]  
0101234.=0031101234.
```

```
[RasSrv::Neighbors]  
dngk1=GnuGK  
dngk2=GnuGK
```

```
[Neighbor::dngk1]  
GatekeeperIdentifier=DutchNational  
Host=dngk1.surfnet.nl  
SendPrefixes=0  
AcceptPrefixes=*  
ForwardResponse=1  
ForwardLRQ=always
```

```
[Neighbor::dngk2]  
GatekeeperIdentifier=DutchNational  
Host=dngk2.surfnet.nl  
SendPrefixes=0  
AcceptPrefixes=*  
ForwardResponse=1  
ForwardLRQ=always
```

```
[Gatekeeper::Auth]  
AliasAuth=required;RRQ  
default=allow
```

```
[RasSrv::RRQAuth]  
; Voorgedefinieerde Accounts
```

```
; kamer1@scenario1.nl ; 0031101234100  
; wijzig het IP adres in het  
; publieke IP adres van het videoconferentieapparaat  
0031101234100=sigip:10.10.10.50:1720
```

```
; gebruiker1@scenario1.nl ; 0031101234200  
; gebruiker1 mag vanuit alle IP adressen registreren  
0031101234200=allow
```