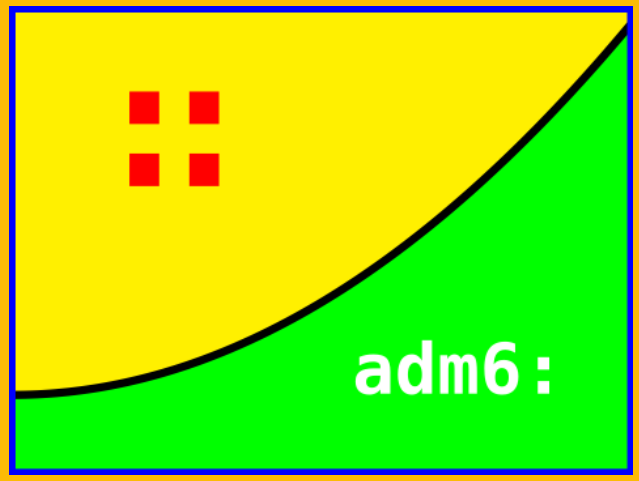
IPv6 – Paketfilter mit Python generieren



Johannes Hubertz

hubertz-it-consulting GmbH

Univention@CeBIT, 7. 3. 2012

adm6: Managementsummary

IPv6-Netzwerksicherheit für **alle Systeme** im **Unternehmen**

Zukunft: IPv6 ist die **Zukunft** auch Ihres Netzwerks!

Verteilt: **Alle Geräte** im Unternehmen mit IPv6-Paketfiltern

Flexibel: **Beliebige Betriebssysteme** und Filterarchitekturen

Zentral: **Einfache Administration** von einem Gerät aus

Nutzen: Nur erwünschter, **nutzbringender IPv6-Datenverkehr**

Redite: **Freie Software** $\rightarrow$ Wirtschaftlichkeit, Investitionssicherheit

Fazit: An der Zukunft führt kein Weg vorbei –

mit adm6: wird Ihr Weg etwas sicherer!

Was zu zeigen ist . . .

Vorstellung – Wer zeigt hier was?

Motivation – Warum das alles?

Ein Konzept

Drei Schritte: Lesen, Kreuzprodukt, Generierung

Ausblick

Quellen und Hinweise

Vorstellung: hubertz-it-consulting GmbH

Erkenntnisse aus dem Berufsleben (seit 1980)

Bellovin and Cheswick: Firewalls and Internet Security, 1994

Fazit: Keep it simple!

Etwas Erfahrung war Voraussetzung

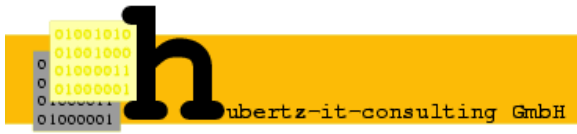
Gründung am 8. August 2005, Sitz in Köln

Geschäftsinhalt: Dienstleistungen im Umfeld der IT-Sicherheit

Logo: Johannes Hubertz Certificate Authority als ASCII-Bitmuster

Diese Bits finden sich in einigen 10^4 X.509 Anwenderzertifikaten bei der Kundschaft in der Seriennummer wieder

Wir sind käuflich ;-)



Einst träumte ich . . . (2002)

Wer Visionen hat, soll zum Arzt gehen

(Helmut Schmidt)

Definitionen in ASCII-Dateien: (Name, Adresse, Kommentar)

Filterregeln in ASCII-Dateien: (src, dest, proto, port, action, cmt)

Erledigt für IPv4: `http://sspe.sourceforge.net` (2003)

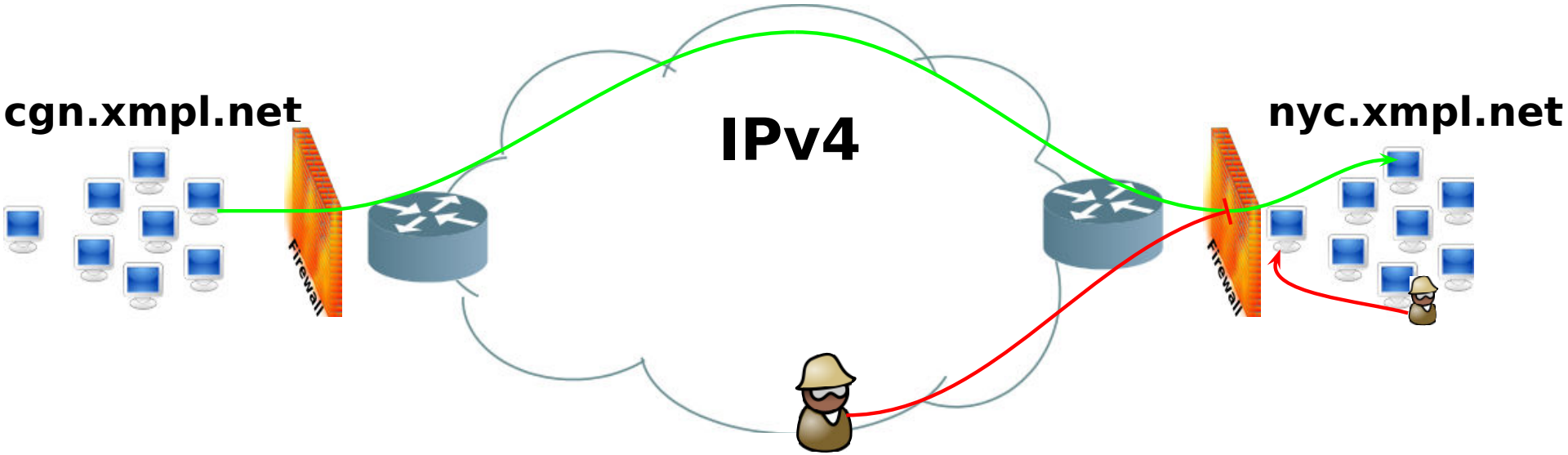
implementiert in Shell und Perl, etwas schwierig für Einsteiger

bei mehreren Kunden erfolgreich im Einsatz

regelmäßig Downloads bei sf.net

Es war einmal ein **IPv4** mit Firewalls und internen . . .

Alles wird gut?



Mit IPv6 wird **alles** anders!

IPv6 . . .

- ist genauso sicher wie IPv4
- ist genauso unsicher wie IPv4
- bietet keinen fragwürdigen Schutz durch NAT
- ist immer Ende zu Ende Kommunikation
- wird genutzt, machmal sogar, ohne dass man es bemerkt
- bietet die gleichen Applikationen und Schwachstellen wie IPv4

Ergo wollen wir keinen ungefilterten Verkehr in unserem Netz!

IPv6 filtern, wo denn?

Menschen mit einer neuen Idee gelten so lange als Spinner,
bis sich die Sache durchgesetzt hat. (Mark Twain)

Wir filtern auf der Firewall, da ist alles sicher!

Wir filtern auf der Firewall und auf den Routern, da ist alles sicher!

auf der Firewall, auf den Routern, auf den Servern, da ist alles sicher!

Wirklich sicher?

Warum nicht auf jedem Gerät?

Zuviel Aufwand? Mit Sicherheit nicht, wenn die Geräte

- über eine sichere Methode verfügen, Kommunikation zu betreiben
- über eine sichere Methode verfügen, Konfiguration zu bearbeiten
- administrativ zu einem Hoheitsbereich gehören

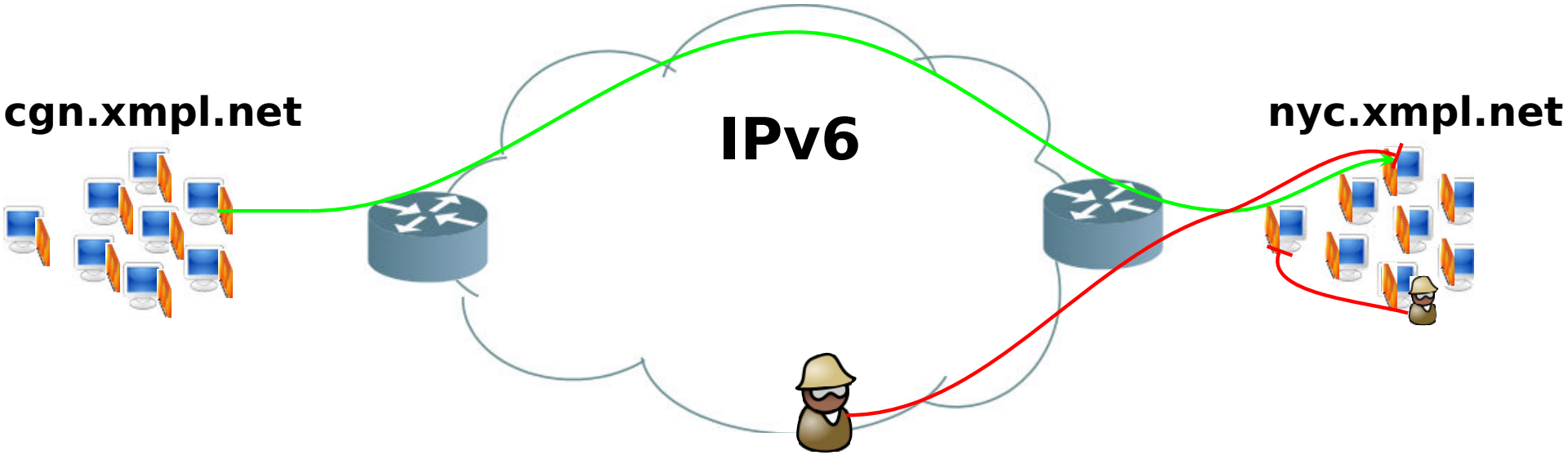
Wir bevorzugen es, auf jedem Gerät zu filtern. . . **wirklich!** . . .

überall!

IPv6 filtern, womit denn?

system	filter	command
Linux	NetFilter	ip6tables
OpenBSD	pf	pf, pf.conf, rc.local
Free- u. NetBSD	ipfilter	ipf
Win XP/SP3	onboard	netsh firewall . . .
Win 7	onboard	netsh advfirewall . . .
IOS 12.+	cisco-acl	access-list . . .
. . .	. . .	. . .

adm6: Eine Idee wird zum Konzept . . .



adm6: Fünfpunktekonzept

Jedes Gerät nutzt einen internen Paketfilter!

1. Alle Paketfilter werden zentral erzeugt und verwaltet
2. Alle Hosts, Router, Firewalls im Netz mit Paketfiltern betreiben
3. Berechnungsgrundlage: Interface- und Routinginformationen
4. Definition aller **Kommunikatoren** (Namen, Adressen)
5. Definition(en) aller **Kommunikationen** (Regelsatz)

Nur erlaubter Netzwerkverkehr bleibt übrig!

adm6: Drei Schritte . . .

Lesen aller Parameter

Kreuzprodukt bilden

Generierung pro Gerät

adm6: Datei- und Verzeichnisstrukturen

```
.adm6.conf
adm6

adm6/bin/
adm6/desc/
adm6/etc/

adm6/desc/adm6/
adm6/desc/ns/
adm6/desc/sfd/
adm6/desc/r-ex/
adm6/desc/obi-lan/

adm6/desc/ns/00-rules.admin
adm6/desc/ns/mangle-startup
adm6/desc/ns/mangle-endup
adm6/desc/ns/hostnet6
adm6/desc/ns/interfaces
adm6/desc/ns/routes

adm6/desc/sfd/00-rules.admin
adm6/desc/sfd/hostnet6
adm6/desc/sfd/interfaces
adm6/desc/sfd/routes

adm6/desc/r-ex/00-rules.admin
adm6/desc/r-ex/hostnet6
adm6/desc/r-ex/interfaces
adm6/desc/r-ex/routes

adm6/desc/obi-lan/00-rules.admin
adm6/desc/obi-lan/mangle-startup
adm6/desc/obi-lan/mangle-endup
adm6/desc/obi-lan/hostnet6
adm6/desc/obi-lan/interfaces
adm6/desc/obi-lan/routes

adm6/etc/00-rules.admin
adm6/etc/Debian-footer
adm6/etc/Debian-header
adm6/etc/hostnet6
adm6/etc/OpenBSD-footer
adm6/etc/OpenBSD-header
```

adm6: Globale Konfiguration

~/.adm.conf liefert:

- **Software Version**
- **Liste aller Gerätenamen**
- **Betriebssystem jeden Gerätes**
- **Aktivitäts-Status jeden Gerätes**
- **ssh-Adresse jeden Gerätes**
- **Forward-Status jeden Gerätes**
- **Asymmetrisches Routing jeden Gerätes**

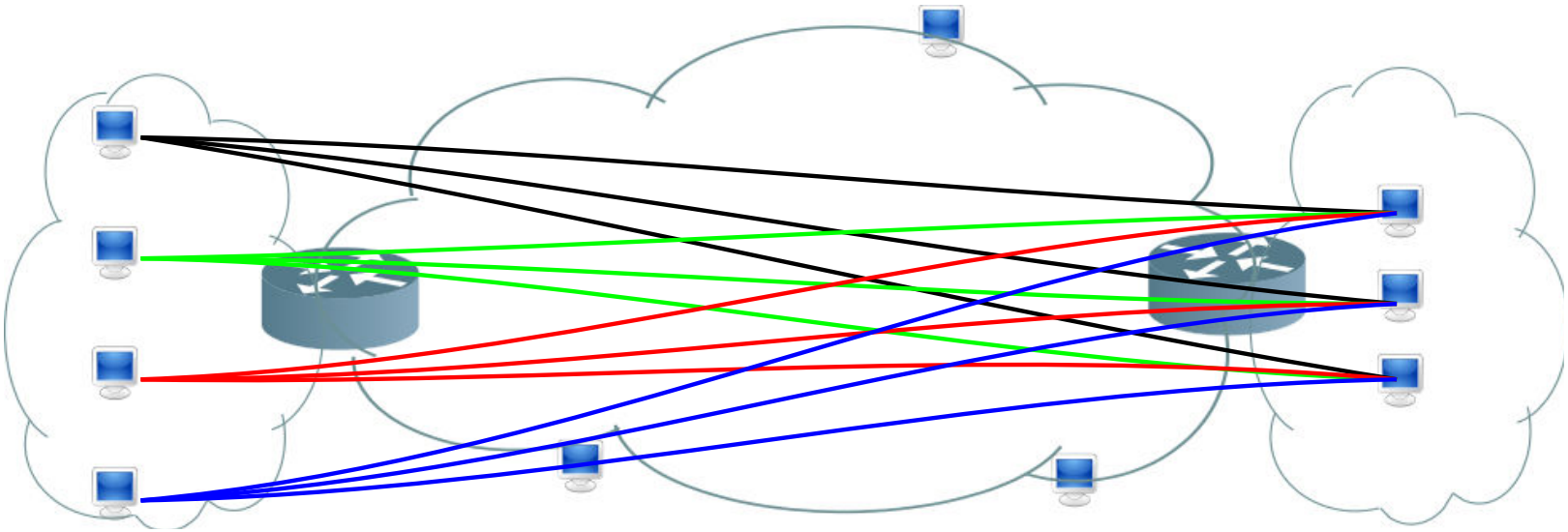
hostnet6 – Namen, Netze und Gruppen

```
# hostnet6      part of adm6                                  # hosts, networks and groups
# name          CIDR address                                  # comment
#                                                             #
any             2000::/3                                      # anybody outside and inside
#                                                             #
admin           2001:db8:f002:2::23/128                       # 1st adminstrators workstation
admin           2001:db8:f002:3::23/128                       # 2nd adminstrators workstation
#
ns              2001:db8:f002:1::53/128                       # 1st domain name server
ns              2001:db8:f002:2::53/128                       # 2nd domain name server
ns              2001:db8:f002:3::53/128                       # 3rd domain name server
www             2001:db8:f002:3::80/128                       # internet web server
intra           2001:db8:f002:1::443/128                      # intranet web server
#
office-cgn      2001:db8:f002:2::/64                          # office cologne
office-muc      2001:db8:f002:3::/64                          # office munich
office-bln      2001:db8:f002:7::/64                          # office berlin
#
fw-i            2001:db8:f002:2::1/128                        # firewall internal view
fw-e            2001:db8:f002:1::2/128                        # firewall external view
#
r-mine          2001:db8:f002::2/128                          # my router to r-isp
r-mine-i        2001:db8:f002:1::1/128                        # my router to r-isp
r-isp-e         2001:db8:abba::1/128                          # ISP routers ISP-side
r-isp           2001:db8:f002::1/128                          # ISP router to r-mine
#
ripe-net        2001:610:240:22::c100:68b/128                 # ripe.net web-server
www-kame-net    2001:200:dff:fff1:216:3eff:feb1:44d7/128      # orange.kame.net
#
# EOF
```

00-rules.admin – Filterregeln (nutzt **hostnet6**)

```
# rules.admin    part          of       adm6
#
# source         destin        proto    port    action   options # comment or not
#
admin            ns            tcp      ssh     accept
admin            ns            udp      53      accept   INSEC NOSTATE # for debug
any              ns            udp      53      accept   NOSTATE # faster without
admin            www           tcp      80      accept
#
office-cgn       any           tcp      80      accept
office-cgn       any           tcp      443     accept
office-cgn       office-muc    ipv6     all     accept
#
office-muc       office-cgn    ipv6     all     accept
any              office-cgn    icmpv6   all     accept
#
# EOF
```

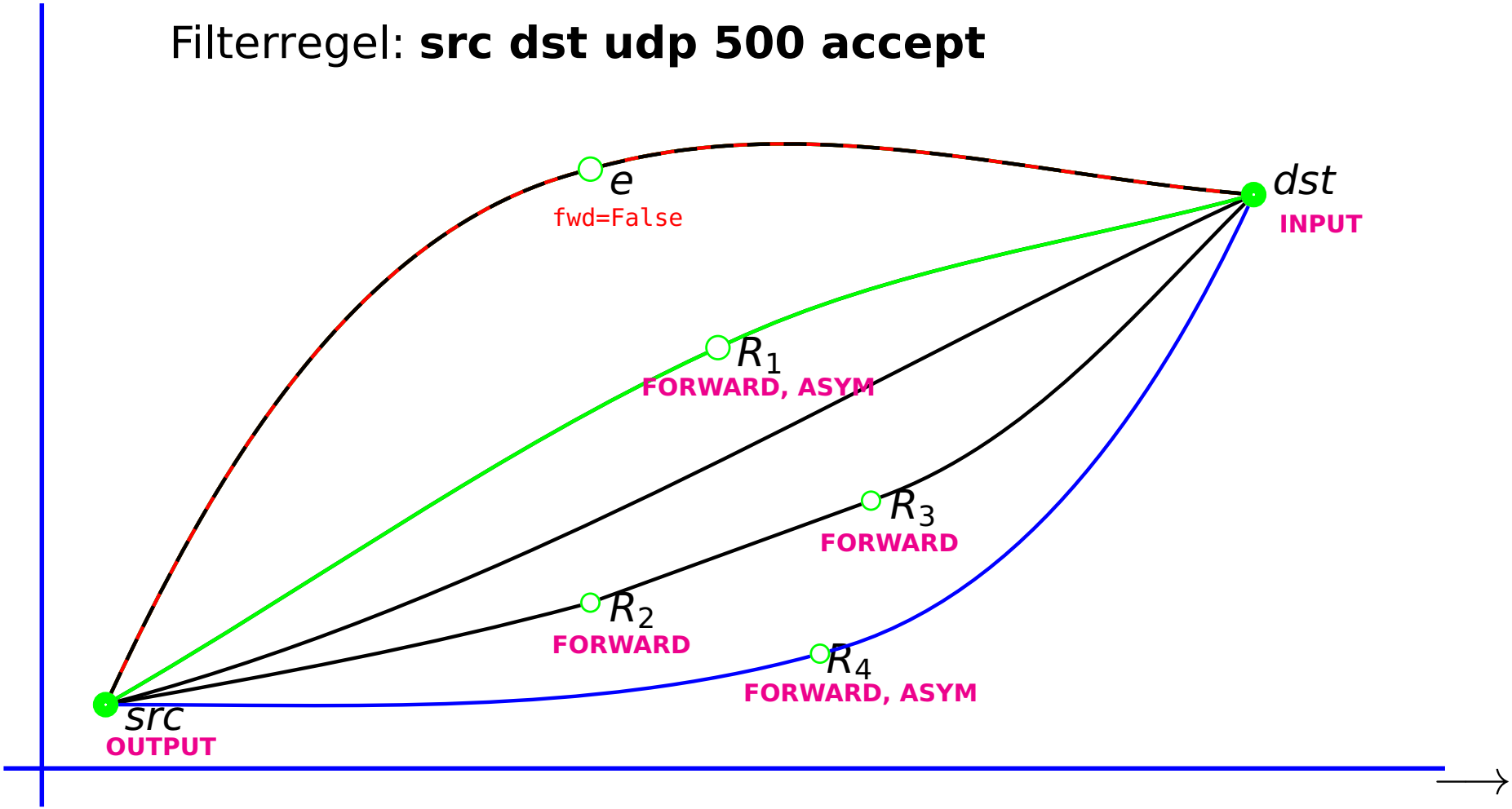
IPv6: Firma mit zwei Standorten



Wollen Sie das händisch konfigurieren?

adm6: Wege durchs Netz

Filterregel: **src dst udp 500 accept**



adm6: Protokolle

1. Manche Protokolle sind unidirektional:

Protokoll	**Besonderheiten**
IPv6	beliebige Quellen und Ziele **::**
ICMPv6	beliebige Quellen und Ziele **::**
Multicasts	Ziel immer auf Linklocal **ff00::/8**
ipencap, ipip	Routingheader, Ziele aus **2000::/3**

2. Andere Protokolle sind bidirektional:

Protokoll	**Besonderheiten**
tcp, udp	beliebige Quellen und Ziele **::**

d.h. es gibt zugehörige Antwortpakete.

adm6: Optionen auf Regeln

Option	**Bedeutung**	fertig
NOIF	Unterdrückung der Interfaceangabe	✓
NONEW	nur „ESTABLISHED, RELATED“ generieren	✓
NOSTATE	Unterdrückung Statefull Inspection	✓
FORCED	IN, OUT, FORWARD unabhängig von Interface- und Routing-Informationen	✓
INSEC	Quellport kleiner 1024 zulassen	✓
NOFORWARD	keinesfalls FORWARD	
LOG	zusätzlich Pakete loggen	
20110615	Ab 15. 6. 2011 nicht mehr generieren	

adm6: Drei Schritte . . .

Lesen aller Parameter

Kreuzprodukt bilden

Generierung pro Gerät

Möglichst **systemunabhängige** Programmierung

Notwendige Informationen pro Gerät:

1. OS-Name bzw. Filterarchitektur
2. OS-spezifische Header- und Footer
3. Interface- und Routinginformationen
4. Host- und Netzdefinitionen
5. Regelsatz (evtl. Geräteabhängig)
6. evtl. Zusätze fürs Shellscript (paket-mangling, QoS)

Realisierung in zwei Objektklassen:

IPv6_Filter: generiert Shellscript aus den Bausteinen (2,6)

IPv6_Filter_Rule: erzeugt jeweiligen Filter pro Regel (1,3,4,5) (System-abhängig)!

Debian Header

```
#!/bin/bash
echo "*********************************************************************"
echo "##                                                                 ##"
echo "##   a d m 6    -  a device manager for IPv6 packetfiltering        ##"
echo "##                                                                 ##"
echo "##   version:      0.1                                           ##"
echo "##                                                                 ##"
echo "##   device-name:  cccccc                                        ##"
echo "##   device-type:  Debian GNU/Linux                              ##"
echo "##                                                                 ##"
echo "##   date:         dddddd                                        ##"
echo "##   author:       Johannes Hubertz, hubertz-it-consulting GmbH  ##"
echo "##                                                                 ##"
echo "##   license:      GNU general public license version 3          ##"
echo "##                     or any later  version                       ##"
echo "##                                                                 ##"
echo "*********************************************************************"
POLICY_D='DROP'
I6='/sbin/ip6tables '
IP6I='/sbin/ip6tables -A   input___new '
IP6O='/sbin/ip6tables -A   output__new '
IP6F='/sbin/ip6tables -A   forward_new '
CHAINS="$CHAINS input__"
CHAINS="$CHAINS output_"
CHAINS="$CHAINS forward"
for chain in $CHAINS
do
        /sbin/ip6tables -N ${chain}_act >/dev/null 2>/dev/null
        /sbin/ip6tables -N ${chain}_new
done
$I6 -P   INPUT $POLICY_D
$I6 -P  OUTPUT $POLICY_D
$I6 -P FORWARD $POLICY_D
# do local and multicast on every interface
LOCAL="fe80::/10"
```

Debian Footer part I

```
#ICMPv6types="${ICMPv6types} destination-unreachable"
ICMPv6types="${ICMPv6types} echo-request"
ICMPv6types="${ICMPv6types} echo-reply"
ICMPv6types="${ICMPv6types} neighbour-solicitation"
ICMPv6types="${ICMPv6types} neighbour-advertisement"
ICMPv6types="${ICMPv6types} router-solicitation"
ICMPv6types="${ICMPv6types} router-advertisement"
for icmptype in $ICMPv6types
do
        $IP6I -p ipv6-icmp --icmpv6-type $icmptype -j ACCEPT
        $IP6O -p ipv6-icmp --icmpv6-type $icmptype -j ACCEPT
done
$IP6I -p ipv6-icmp --icmpv6-type destination-unreachable -j LOG  --log-prefix "unreach: " \
                   -m limit --limit 30/second --limit-burst 60
$IP6I -p ipv6-icmp --icmpv6-type destination-unreachable -j ACCEPT
#
CHAINS=""
CHAINS="$CHAINS input___"
CHAINS="$CHAINS output_"
CHAINS="$CHAINS forward"
#set -x
for chain in $CHAINS
do
        /sbin/ip6tables -E "${chain}_act" "${chain}_old"
        /sbin/ip6tables -E "${chain}_new" "${chain}_act"
done
#
$I6 -F INPUT
$I6 -A INPUT   -m rt --rt-type 0 -j LOG --log-prefix "rt-0: " -m limit --limit 3/second --limit-burst 6
$I6 -A INPUT   -m rt --rt-type 0 -j DROP
$I6 -A INPUT   -m rt --rt-type 2 -j LOG --log-prefix "rt-2: " -m limit --limit 3/second --limit-burst 6
$I6 -A INPUT   -m rt --rt-type 2 -j DROP
$I6 -A INPUT  -i lo -j ACCEPT
$I6 -A INPUT   --jump input___act
#
```

Windows XP Header

```
@echo off                                                                    1
echo "adm6: test-batch header file for device: wxp-jh                 "     2
echo "adm6: created on:  2011-06-02 15:29                            "     3
rem ############################################################################ 4
rem disable privacy extensions                                               5
rem                                                                          6
netsh interface ipv6 set global randomizeidentifiers=disabled                7
netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent 8
netsh interface ipv6 set privacy state=disabled store=persistent             9
rem ############################################################################ 10
rem disable teredo tunnels                                                   11
rem                                                                          12
netsh interface 6to4 set state state=disabled undoonstop=disabled            13
netsh interface isatap set state state=disabled                              14
netsh interface teredo set state type=disabled                               15
rem                                                                          16
rem ############################################################################ 17
rem ############################################################################ 18
```

Eine Regel und was daraus wird: **Debian**

```
# ------------------------------------------------------------------------ #
# Rule-Nr        : 3                                                       #
# Pair-Nr        : 1                                                       #
# System-Name    : r-ex                                                    #
# OS             : Debian                                                  #
# RuleText       : ['any', 'ns', 'udp', '53', 'accept', 'NOSTATE']         #
# Source         : 2000::/3                                                #
# Destin         : 2001:db8:23:1::23/128                                   #
# Protocol       : udp                                                     #
# sport          : 1024:                                                   #
# dport          : 53                                                      #
# Action         : accept                                                  #
# nonew          : False                                                   #
# noif           : False                                                   #
# nostate        : True                                                    #
# insec          : False                                                   #
# i_am_s         : None                                                    #
# i_am_d         : None                                                    #
# travers        : True                                                    #
# source-if      : eth3                                                    #
# source-rn      : 10                                                      #
# src-linklocal  : False                                                   #
# src-multicast  : False                                                   #
# destin-if      : eth1                                                    #
# destin-rn      : 1                                                       #
# dst-linklocal  : False                                                   #
# dst-multicast  : False                                                   #
/sbin/ip6tables -A   forward_new  -i eth3 -s 2000::/3 -d 2001:db8:23:1::23/128 \
                          -p udp --sport 1024: --dport 53 -j ACCEPT
/sbin/ip6tables -A   forward_new  -o eth1 -d 2000::/3 -s 2001:db8:23:1::23/128 \
                          -p udp --dport 1024: --sport 53 -j ACCEPT
```

adm6: aus der Praxis

Betrieb – Erfahrung

adm6: Betrieb – 24/7

If the facts don't fit the theory, change the facts.

(Albert Einstein)

Start im September 2010 auf 2 Linuxsystemen (web, dns, mail)

Nutzung von `he.net/certification` und `lg.he.net` (Tests)

Regeln seit Oktober 2010 unverändert

Verbesserungen in Header und Footer bis Dezember 2010

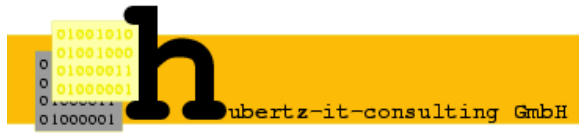
Start auf Linuxrouter im Januar 2011 mit gleichen Regeln

Experimente mit OpenBSD und Win(xp) seit 2011

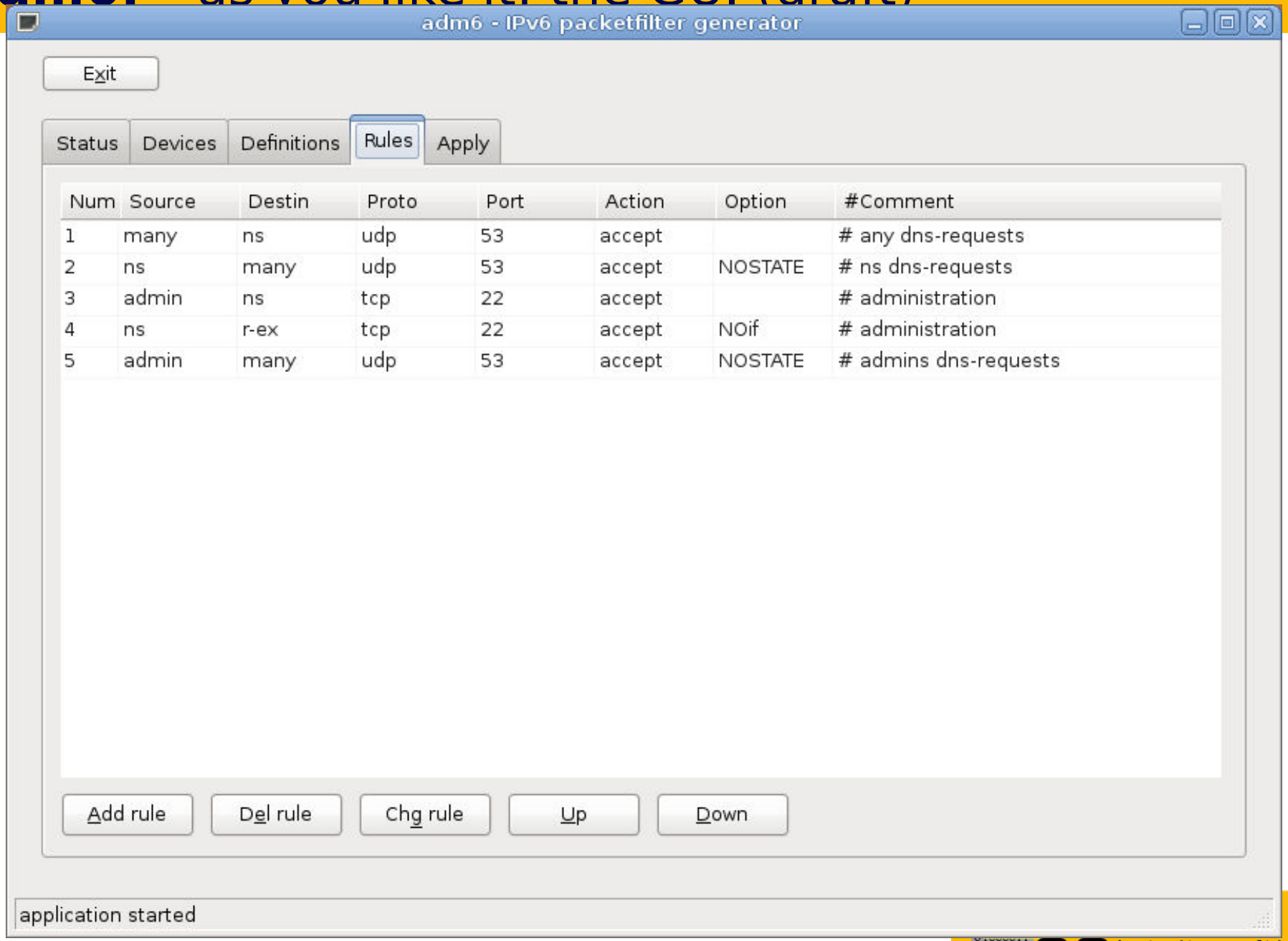
Asymmetrisches Routing ab August 2011

Jan. 2012: python-paramiko zum Lesen, scp zur Verteilung

Jan. 2012: ~/adm6/.git, commit zu jeder Erzeugung / Verteilung



adm6: – as you like it: the GUI (draft)



Quellen und Anregungen (Auszug)

... only a few of more than 200 ...
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462 IPv6 Stateless Address Autoconfiguration
RFC 2463 Internet Control Message Protocol for the Internet Protocol Version 6 (IPv6) Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
RFC 3756 IPv6 Neighbor Discovery (ND) Trust Models and Threats
RFC 3775 Mobility Support in IPv6
RFC 3971 SEcure Neighbor Discovery (SEND)
RFC 3972 Cryptographically Generated Addresses (CGA)
RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6
RFC 4443 Internet Control Message Protocol for the Internet Protocol Version 6 (IPv6) Specification
RFC 4861 Neighbor Discovery for IPv6
RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls
RFC 5095 Deprecation of RH0

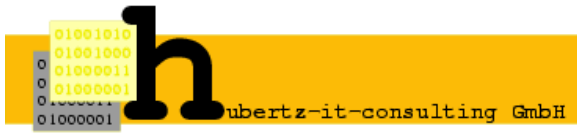
Linux:
http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html
OpenVPN-tunnelbroker: http://blog.ghitr.com/index.php/archives/673
http://www.6net.org/publications/presentations/strauf-openvpn.pdf

Books:
IPv6, Sylvia Hagen, Sunny Edition, 2. Auflage, ISBN 978-3-9522842-2-2
IPv6 in Practice, Benedikt Stockebrand, Springer, ISBN 978-3-540-24524-7
IPv6 Security, Scott Hogg, Eric Vyncke, Cisco Press, ISBN 1587055942
Deploying IPv6 Networks, Ciprian Popoviciu et.al., Cisco Press, ISBN 1587052105

Tests:
http://freeworld.thc.org/thc-ipv6/
http://lg.he.net/

Security:
http://www.wecon.net/files/48/GUUG-RT_WEST2010-SvI.pdf
http://seanconvery.com/ipv6.html

Lernen:
http://owend.corp.he.net/ipv6/IPv6%20Tutorial/Half%20Day%20Intro.pdf
http://owend.corp.he.net/ipv6/
http://ipv6.he.net/certification/



adm6: Zeit zum Dialog!

Kompetente und kompatible

Schlangenbändiger gesucht!

Noch Fragen?

Ich bedanke mich für Ihre Aufmerksamkeit

hubertz-it-consulting GmbH jederzeit zu Ihren Diensten

Ihre Sicherheit ist uns wichtig!

Frohes Schaffen

Johannes Hubertz

`it-consulting _at_ hubertz dot de`

$H\alpha \in \{$ `kompetenzspektrum.de` $\}$

adm6: EVOLVIS Repository

`git clone https://evolvis.org/anonscm/git/adm6/adm6.git`

`http://www.hubertz.de/papers/20120301-p.pdf`

powered by LaTeX 2ε and PSTricks