Technische Dokumentation

Umsetzung eines IPv6-Netzwerksegmentes mit Internetanbindung für die FastForward GmbH

Jahresprojekt der FS22 HHBK, 20. April 2016

Geplant und umgesetzt von:
Kilian Engelhardt
Mirko Großmann
Tom Vogler

Inhaltsverzeichnis

Anmerkungen **1**

Informationen **2**
- Verwendete Hardware . . . 2
- DNS . . . 2
- SixXS . . . 2
- Adresskonzept . . . 2
- Netzwerkplan . . . 2

Router: Konfiguration **2**

Switch: Konfiguration **4**

Hypervisor **5**
- Installation . . . 5
- Konfiguration . . . 6
  - libvirt . . . 6
  - Netzwerk . . . 6

Linux-Server **7**
- Installation . . . 7
- Konfiguration . . . 8
  - Netzwerk . . . 8

Domain Controler **8**
- Installation . . . 8
- Konfiguration . . . 9

Windows Client **9**
- Installation . . . 9
- Konfiguration . . . 9

Tests **9**
- Erreichbarkeit intern . . . 9
- Erreichbarkeit extern . . . 10
  - Allgemeine Erreichbarkeit . . . 10
  - Erreichbarkeit Webserver . . . 10
  - Erreichbarkeit Mailserver . . . 11
- Firewall . . . 11

Anmerkungen

Alle im Projekt verwendeten Passwörter wurden aus Datenschutzgründen in der Dokumentation durch die Zeichenfolge „password123“ ersetzt. Alle Kommandoaufrufe wurden zur Vereinfachung als Benutzer root in einer Bash-Shell ausgeführt.[1] Folgt einer Zeile mit einem Kommandoaufruf das Zeichen \ (Backslash), so gehört die nächste Zeile ebenfalls zum Kommandoaufruf.[2]

Darstellung von Kommandozeilenaufrufen:

```
> Kommandozeilenaufrufe werden in einem weißen Kasten in Monospace mit einem \
  vorangestellten > (Größer-als-Zeichen) dargestellt.
```

Darstellung von Konfigurationen:

```
1 Konfigurationen werden ähnlich wie Kommandozeileaufrufe in einem weißen Kasten
2 dargestellt, jedoch mit nummerierten Zeilen.
```

[1] Um Verwechslungen in der Dokumentation durch ständiges Wechseln zwischen einem Normalbenutzer und dem Superuser, sowie die Verwendung von sudo-Aufrufen und unnötige Komplikationen mit Zugriffsrechten zu vermeiden.

[2] Auszug aus man bash: „A non-quoted backslash (\) is the escape character. It preserves the literal value of the next character that follows, with the exception of <newline>. If a <newline> pair appears, and the backslash is not itself quoted, the <newline> is treated as a line continuation (that is, it is removed from the input stream and effectively ignored).“

Informationen

Verwendete Hardware

- Router: Cisco 2801
- Switch: Cisco C2960
- no-name Server:

CPU AMD Phenom X2 II 965 4x 3,4Ghz
RAM 4x Kingston DDR3-1333Mhz 4GB
SSD OCZ-VERTEX3 60GB
HDD Hitachi HDS72105 500GB
LAN 4x Gigabit-Ethernet

- Linux-Server

vCPUs 1
RAM 4GB
HDD 100GB

- Domain Controler

vCPUs 3
RAM 8GB
HDD 300GB

DNS

Folgende DNS-Einstellungen wurden vorgenommen, um den Linux-Server aus dem Internet über die Domain FASTFORWARD.HHBK.DE erreichbar zu machen.

```
fastforward.hhbk.de.    A    212.72.180.241
fastforward.hhbk.de.    AAAA 2001:4dd0:fc0b:a::4
fastforward.hhbk.de.    MX   fastforward.hhbk.de
```

SixXS

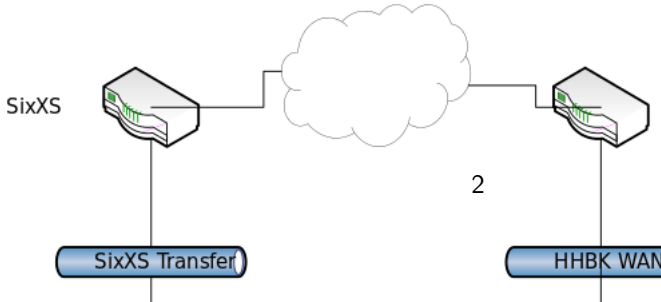
Adresskonzept

	LAN: VLAN 20	DMZ: VLAN 10
Router	2001:4dd0:fc0b:f4::1/128	2001:4dd0:fc0b:a::1/128
Switch	2001:4dd0:fc0b:f4::2/128	2001:4dd0:fc0b:a::2/128
Hypervisor	2001:4dd0:fc0b:f4::3/128	2001:4dd0:fc0b:a::3/128
Linux-Server	2001:4dd0:fc0b:a::4/128	
Domain Controler	2001:4dd0:fc0b:f4::5/128	
Client01	2001:4dd0:fc0b:f4::a/128	
Client02	2001:4dd0:fc0b:f4::b/128	
Client03	2001:4dd0:fc0b:f4::c/128	

Netzwerkplan

Router: Konfiguration

Abweichend von der einleitenden Anmerkung wurden folgende Befehle unter Ciscos iOS verwendet, um die Konfiguration des Routers vorzunehmen.



```
#Basics
r1#conf t
r1(config)#enable secret password123
r1(config)#enable password password123
r1(config)#ipv6 unicast-routing
r1(config)#ip name-server 8.8.8.8

#Vlan Deklaration
r1#vlan database
r1(vlan)#vlan 10
r1(vlan)#vlan 20
r1(vlan)#apply
r1(vlan)#exit

#Subinterface vlan 10
r1(config)#interface FastEthernet0/1.10
r1(config-subif)#description subinterface vlan 10
r1(config-subif)#encapsulation dot1Q 10
r1(config-subif)#ipv6 address 2001:4dd0:fc0b:a::1/64
r1(config-subif)#no shutdown
r1(config-subif)#exit

#Subinterface vlan 20
r1(config)#interface FastEthernet0/1.20
r1(config-subif)#description subinterface vlan 20
r1(config-subif)#encapsulation dot1Q 20 native
r1(config-subif)#ipv6 address 2001:4dd0:fc0b:f4::1/64
r1(config-subif)#no shutdown
r1(config-subif)#exit

#Interface ins Schulnetz
r1(config)#interface fastethernet 0/0
r1(config-if)#ip address 212.72.180.241 255.255.255.224
r1(config-if)#ip default-gateway 212.72.180.225
r1(config-if)#no shutdown
r1(config-if)#exit

#SSH
r1(config)#ip domain-name fastforward.hhbk.de
r1(config)#crypto key generate rsa general-keys modulus 1024
r1(config)#username admin privilege 15 secret password123
r1(config)#line vty 0 4
r1(config-line)#transport input telnet ssh
r1(config-line)#login local
r1(config-line)#end

#Routing
r1(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0/0
r1(config)#ipv6 route 2001:4dd0:fc0b:a::/64 FastEthernet0/1.10
r1(config)#ipv6 route 2001:4dd0:fc0b:f4::/64 FastEthernet0/1.20

r1(config)#interface Tunnel61
r1(config-if)#description 6in4 tunnel to SixXS
r1(config-if)#no ip address
r1(config-if)#ip tcp adjust-mss 1420
r1(config-if)#ipv6 address 2001:4dd0:ff00:147f::2/64
r1(config-if)#ipv6 enable
r1(config-if)#tunnel source fastethernet 0/0
r1(config-if)#tunnel destination 78.35.24.124
r1(config-if)#tunnel mode ipv6ip
r1(config-if)#exit
r1(config)#ipv6 route ::/0 Tunnel61

#Tunnel Prüfen
r1#show ip interface tunnel61
r1#show ipv6 interface tunnel61
```

Konfiguration der Firewall:

```
#Firewalling
r1(config)#ipv6 access-list from_wan_in
```

```
r1(config-ipv6-acl)#permit icmp any any
r1(config-ipv6-acl)#permit tcp any any eq 22
r1(config-ipv6-acl)#permit tcp any any eq www reflect dmz-wan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq 443 reflect dmz-wan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq smtp
r1(config-ipv6-acl)#evaluate wan-dmz-reflexive
r1(config-ipv6-acl)#evaluate wan-lan-reflexive

r1(config)#interface Tunnel61
r1(config-if)#ipv6 traffic-filter from_wan_in in

r1(config)#ipv6 access-list dmz_in
r1(config-ipv6-acl)#permit icmp any any
r1(config-ipv6-acl)#permit udp any any eq domain reflect wan-dmz-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq 22 reflect wan-dmz-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq www reflect wan-dmz-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq 443 reflect wan-dmz-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq smtp reflect wan-dmz-reflexive timeout 5
r1(config-ipv6-acl)#evaluate dmz-wan-reflexive

r1(config)#interface FastEthernet0/1.10
r1(config-if)#ipv6 traffic-filter dmz_in in

r1(config)#ipv6 access-list lan_in
r1(config-ipv6-acl)#permit icmp any any
r1(config-ipv6-acl)#permit udp any any eq domain reflect wan-lan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq 22 reflect wan-lan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq www reflect wan-lan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq 443 reflect wan-lan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq smtp reflect wan-lan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq ftp reflect wan-lan-reflexive timeout 5
r1(config-ipv6-acl)#permit tcp any any eq ftp-data reflect wan-lan-reflexive timeout 5

r1(config)#interface FastEthernet0/1.20
r1(config-if)#ipv6 traffic-filter lan_in in

r1(config)#interface FastEthernet0/0
r1(config-if)#ip access-group from_wan_in in

r1(config)#do show ipv6 access-list
```

Switch: Konfiguration

Abweichend von der einleitenden Anmerkung wurden folgende Befehle unter Ciscos iOS verwendet, um die Konfiguration des Switches vorzunehmen.

```
#Basic
switch(config)#enable secret Willkommen2016
switch(config)#enable password Willkommen2016
switch(config)#sdm prefer dual-ipv4-and-ipv6
switch(config)#end
switch# reload

#Vlan Deklaration
switch#vlan database
switch(vlan)#vlan 10
switch(vlan)#vlan 20
switch(vlan)#exit

#interface vlan 10
switch(config)#interface range gigabitEthernet f0/1-24
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#end
Switch(config)#interface vlan 10
Switch(config-if)#ipv6 address 2001:4dd0:fc0b:a::2/64
Switch(config-if)#no shut down
Switch(config-if)#exit
```

```
#interface vlan 20
switch(config)# interface range gigabitEthernet f0/25-46
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# end
Switch(config)#interface vlan 20
Switch(config-if)#ipv6 address 2001:4dd0:fc0b:f4::2/64
Switch(config-if)#no shut down
Switch(config-if)# exit

#trunk
switch(config)#interface gigabitEthernet 0/43
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#switchport trunk allowed vlan 10,20

#SSH
Switch(config)#ip domain-name fastforward.hhbk.de
Switch(config)#crypto key generate rsa general-keys modulus 1024
Switch(config)#username admin privilege 15 secret Willkommen2016
Switch(config)#line vty 0 4
Switch(config-line)#transport input telnet ssh
Switch(config-line)#login local
Switch(config-line)#en
```

Hypervisor

Installation

Die Installation erfolgt per graphischen Installationsdialog. Englisch wurde gewählt, da es die Lingua franca in der IT darstellt. Zusätzlich wurde OpenSSH bei der Installation ausgewählt, um den Server ohne graphische Oberfläche aus der Ferne zu administrieren. Insgesamt wurden während der Installation folgende Einstellungen vorgenommen:

Language	Englisch
Territory	Germany
Keyboard	german
Hostname	hypervisor
Domain name	fastforward.hhbk.de
Username	user
Password	password123
Paritioning	Guided: use entire disk
Choose software	Default, OpenSSH
Grub MBR	sdb

Nach der Installation wurde darüberhinaus folgende Software installiert: QEMU-KVM LIBVIRT-BIN VIRTINST.

Konfiguration

libvirt

Zunächst muss der QEMU-Treiber von LIBVIRT konfiguriert werden, damit dieser weiß, mit welchem User QEMU ausgeführt wird.

Konfigurationsdatei: /ETC/LIBVIRT/QEMU.CONF

```
user = "root"
group = "root"
```

Anschließend wird die HDD mit 500GB formatiert und die Volume Group VG0 definiert.

```
> parted /dev/sda
   mklabel GPT
   mkpart primary 1M 100%
   set 1 lvm on
> pvcreate /dev/sda1
> vgcreate vg0 /dev/sda1
```

Die Volume Group VG0 wird verwendet, um den Pool VG0 einzurichten. Die folgende Konfiguration muss erstellt werden, um anschließend mit den aufgeführten Befehlen den Pool zu aktivieren.

Konfigurationsdatei: /ETC/LIBVIRT/QEMU/STORAGE/VG0.XML

```
<pool type='logical'>
        <name>vg0</name>
        <source>
                <device path='/dev/sda1'/>
        </source>
        <target>
                <path>/dev/vg0</path>
        </target>
</pool>
```

```
> virsh pool
-define /etc/libvirt/qemu/storage/vg0.xml
> virsh pool-start vg0
> virsh pool-autostart vg0
```

Netzwerk

Der Hypervisor wurde mit zwei Interfaces an den Switch angebunden. Das Interface ENP4S0 wurde an einen Port mit VLAN 10 angeschlossen und ENP2S0 an einen Port mit VLAN 20. Dadurch ist es später einfacher, die virtuellen Server einem VLAN zuzuordnen (s. Kapitel „Linux-Server“). Für DNS wurde ein Server von Google ausgewählt.

Konfigurationsdatei: /ETC/NETWORK/INTERFACES

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
```

```
iface lo inet loopback

# The primary network interface
auto enp4s0
iface enp4s0 inet manual

      dns-nameservers 2001:4860:4860::8888

auto enp2s0
iface enp2s0 inet manual

      dns-nameservers 2001:4860:4860::8888

auto br0
iface br0 inet manual

iface br0 inet6 static
        bridge_ports    enp4s0
        address 2001:4dd0:fc0b:a::3
        netmask 64
        gateway 2001:4dd0:fc0b:a::1

auto br1
iface br1 inet manual

iface br1 inet6 static
        bridge_ports    enp2s0
        address 2001:4dd0:fc0b:f4::3
        netmask 64
```

Linux-Server

Installation

Die virtuelle Maschine wurde auf dem Hypervisor mithilfe von VIRTINST und folgendem Befehl initialisiert.

```
> virt
-install --connect qemu:///system --hvm
 --name webserver --ram 4096 --vcpus 1 \
  --disk pool=vg0,size
=100,bus=virtio,cache=none,sparse=false \
  --cdrom=/root/isos/ubuntu
-16.04-server-amd64.iso --os-type linux \
  --network bridge=br0,model=virtio \
  --graphics vnc,port=10123,listen
=0.0.0.0,keymap=de,password=password123 \
  --boot cdrom
```

Über die IP des Hypervisors und den Port 10123 wurde eine Verbindung per VNC hergestellt, um anschließend die Installation per graphischem Installationsdialog durchzuführen. Englisch wurde gewählt, da es die Lingua franca in der IT darstellt. Zusätzlich wurde OpenSSH bei der Installation ausgewählt, um den Server ohne graphische Oberfläche aus der Ferne zu administrieren. Insgesamt wurden während der Installation folgende Einstellungen vorgenommen:

Language	Englisch
Territory	Germany
Keyboard	german

Hostname	webserver
Domain name	fastforward.hhbk.de
Username	user
Password	password123
Paritioning	Guided: use entire disk
Choose software	Default, OpenSSH
Grub MBR	vda

Nach der Installation wurde darüberhinaus folgende Software installiert: APACHE2 POSTFIX.

Konfiguration

Nach der Installation von Apache wurde die Defaultwebseite durch eine ersetzt, die „Hello World!“ ausliefert.

Konfigurationsdatei: /VAR/WWW/HTML/INDEX.HTML

```
Hello World!
```

Während des Installationsdialoges von Postfix wurde „Internet with Smarthost“ gewählt. Der SMTP-Server bleibt unkonfiguriert. Als Domain wird „fastforward.hhbk.de“ angegeben.

Netzwerk

Konfigurationsdatei: /ETC/NETWORK/INTERFACES

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens3
iface ens3 inet manual

iface ens3 inet6 static
        address     2001:4dd0:fc0b:a::4
        netmask     64
        gateway     2001:4dd0:fc0b:a::1

      dns-nameservers 2001:4860:4860::8888
```

Domain Controler

Installation

Die virtuelle Maschine wurde auf dem Hypervisor mithilfe von VIRTINST und folgendem Befehl initialisiert.

```
> virt
-install --hvm --connect qemu:///system
 --name win2012 --ram 8192 --vcpus 2 \
  --disk pool=vg0,size
=300,bus=virtio,cache=none,sparse=false \
  --disk path=/root/isos
/virtio-win.iso,device=cdrom,perms=ro \
  --cdrom /root/isos/win2012r2.iso \
  --os-type windows \
  --network bridge=br0,model=virtio \
  --graphics vnc,port=10234,listen
=0.0.0.0,keymap=de,password=password123 \
  --boot cdrom,hd,menu=on
```

Anschließend wurde sich per VNC verbunden, um den Domain Controler per graphischem Installationsdialog zu installieren. Dabei wurde eine Installation mit graphischer Oberfläche gewählt, da dies der üblichen Administrationsweise unter Windows entspricht. Während der Installation müssen über die zusätzlich eingebundene CD „virtio-win“ die Treiber für das Netzwerk (NETKVM > WIN2012R2 > AMD64) und die Festplatte (VIOSTOR > WIN2012 R2 > AMD64)installiert werden. Bei der Partitionierung wurde die gesamte Festplatte gewählt und abschließend dem Administrator das Passwort „password123“ gegeben.

Konfiguration

Windows Client

Installation

Konfiguration

Tests

Erreichbarkeit intern

Mit dem folgenen Skript wurde die allgemeine Erreichbarkeit der Server aus dem LAN getestet.

Shell-Skript: TEST-PING.SH

```
1  #!/bin/bash
2
3  #killall dhclient
4
5  RIP1="2001:4dd0:fc0b:a::1"
6  RIP2="2001:4dd0:fc0b:f4::1"
7  SIP1="2001:4dd0:fc0b:a::2"
8  SIP2="2001:4dd0:fc0b:f4::2"
9  KVM1="2001:4dd0:fc0b:a::3"
10 KVM2="2001:4dd0:fc0b:f4::3"
11 SRV="2001:4dd0:fc0b:a::4"
12 DC="2001:4dd0:fc0b:f4::5"
13
14 LOG="test-ping_$(date +%Y%d%m).log"
15
16 IP="${RIP1} ${RIP2} ${SIP1} ${SIP2} ${KVM1} ${KVM2} ${SRV} ${DC}"
17
18 echo -e "##########" >> ${LOG}
19 echo -e "Ping-Test $(date +%Y%m%d):\n" >> ${LOG}
20 for i in ${IP}; do
```

```
  ping6 -c 1 ${i} 2> /dev/null
  if [[ $? -eq 0 ]]; then
    echo -e "${i}\t\tworks" >> ${LOG}
  else
    echo -e "${i}\t\tfailed!" >> ${LOG}
  fi
done
echo -e "\n" >> ${LOG}
```

Log-Datei: TEST-PING_20160622.LOG

```
##########
Ping-Test 20160622:

2001:4dd0:fc0b:a::1     works
2001:4dd0:fc0b:f4::1        works
2001:4dd0:fc0b:a::2     works
2001:4dd0:fc0b:f4::2        works
2001:4dd0:fc0b:a::3     works
2001:4dd0:fc0b:f4::3        works
2001:4dd0:fc0b:a::4     works
2001:4dd0:fc0b:f4::5        works
```

Erreichbarkeit extern

Allgemeine Erreichbarkeit

Zum Testen der allgemeinen Erreichbarkeit von extern wurde der Ping-Test an einem Internetanschluss mit Dualstack wiederholt.

```
##########
Ping-Test 20160622:

2001:4dd0:fc0b:a::1     works
2001:4dd0:fc0b:f4::1        works
2001:4dd0:fc0b:a::2     works
2001:4dd0:fc0b:f4::2        works
2001:4dd0:fc0b:a::3     works
2001:4dd0:fc0b:f4::3        works
2001:4dd0:fc0b:a::4     works
2001:4dd0:fc0b:f4::5        works
```

Erreichbarkeit Webserver

Die Erreichbarkeit des Webservers wurde von der Kommandozeile per CURL getestet.

```
> curl -v fastforward.hhbk.de
 * Rebuilt URL to: fastforward.hhbk.de/
 * Hostname was NOT found in DNS cache
 *   Trying 2001:4dd0:fc0b:a::4 ...
 * Connected to fastforward.hhbk.de (2001:4dd0:fc0b:a::4) port 80 (#0)
 > GET / HTTP/1.1
 > User-Agent: curl/7.35.0
 > Host: fastforward.hhbk.de
 > Accept: */*
 >
 < HTTP/1.1 200 OK
 < Date: Wed, 22 Jun 2016 15:03:00 GMT
 * Server
 Apache/2.4.18 (Ubuntu) is not blacklisted
 < Server: Apache/2.4.18 (Ubuntu)
 < Last
-Modified: Mon, 20 Jun 2016 07:40:59 GMT
```

```
< ETag: "d-535b0d3581c7e"
< Accept-Ranges: bytes
< Content-Length: 13
< Content-Type: text/html
<
Hello World!
* Connection #0 to host fastforward.hhbk.de left intact
```

Erreichbarkeit Mailserver

Die Erreichbarkeit des Mailservers wurde von der Kommandozeile per TELNET getestet.

```
> telnet fastforward.hhbk.de 25
 Trying 2001:4dd0:fc0b:a::4...
 Connected to fastforward.hhbk.de.
 Escape character is '^]'.
 220 webserver ESMTP Postfix (Ubuntu)
 HELO fastforward.hhbk.de
 250 webserver
 mail from: <test@test.com>
 250 2.1.0 Ok
 rcpt to: <kilian@fastforward.hhbk.de>
 250 2.1.5 Ok
 subject: test
 Line one
 Line two
 .
 250 2.0.0 Ok: queued as 1BF1B6099B
 quit
 221 2.0.0 Bye
 Connection closed by foreign host.
```

```
> tail /var/mail/kilian
 X-Original-To: kilian@fastforward.hhbk.de
 Delivered-To: kilian@fastforward.hhbk.de
 Received
: from fastforward.hhbk.de (unknown [IPv6
:2a02:908:1251:7160:495e:958d:9e35:f017])
  by webserver
 (Postfix) with SMTP id 1BF1B6099B
  for <kilian@fastforward.hhbk.de
>; Wed, 22 Jun 2016 16:49:47 +0200 (CEST)

 subject: test
 Line one
 Line two
```

Firewall

Mit den folgenden Kommandos wurde getestet, ob die Firewall nicht freigeschaltete Ports blockiert. Dazu wurde auf dem Linux-Server mit NETCAT ein Port geöffnet und von extern geprüft, ob sich zu diesem Port verbunden werden kann.

```
1 #Listening auf dem Linux-Server
2 > netcat -l -p 1337
3
4 #Vom externen Host
5 > telnet 2001:4dd0:fc0b:a::4 1337
6  Trying 2001:4dd0:fc0b:a::4...
```

```
7 telnet: connect to address
  2001:4dd0:fc0b:a::4: Permission denied
```