Lab14 - Vorbereitung 2

Holzer Matthias

[Networkplan 2](#_Toc67001217)

[Addressing Table 2](#_Toc67001218)

[VLAN und Port Mappings 2](#_Toc67001219)

[ACLs Problems 3](#_Toc67001220)

[1. The Specifications are impossible to accomplish 3](#_Toc67001221)

[2. First change is also not doable 3](#_Toc67001222)

[Final Solution for the ACL 4](#_Toc67001223)

[Verification 4](#_Toc67001224)

[Path with hop counts 4](#_Toc67001225)

[DNS with command Line 7](#_Toc67001226)

[PPP 7](#_Toc67001227)

[BGP 8](#_Toc67001228)

[Port Security 9](#_Toc67001229)

[DHCP 9](#_Toc67001230)

[VLANs 10](#_Toc67001231)

[Inter-VLAN routing 11](#_Toc67001232)

[Dynamic, Static and default Routing 11](#_Toc67001233)

[SSH Telnet 12](#_Toc67001234)

[NAT 13](#_Toc67001235)

[ACL 13](#_Toc67001236)

# Networkplan

Diagram

Description automatically generated

# Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| **HQ** | G0/0 | 10.0.1.1 | 255.255.255.0 |
| G0/1 | 192.0.2.1 | 255.255.255.0 |
| S0/0/0 | 10.255.255.1 | 255.255.255.252 |
| S0/0/1 | 10.255.255.253 | 255.255.255.252 |
| S0/1/0 | 209.165.201.1 | 255.255.255.252 |
| **B1** | G0/0.10 | 10.209.10.1 | 255.255.255.0 |
| G0/0.20 | 10.209.20.1 | 255.255.255.0 |
| G0/0.**30** (encapsulation dot1q **42)** | 10.209.**42**.1 | 255.255.255.0 |
| G0/0.99 | 10.209.99.1 | 255.255.255.0 |
| S0/0/0 | 10.255.255.2 | 255.255.255.252 |
| **B1-S1** | VLAN 99 | 10.209.99.21 | 255.255.255.0 |
| **B1-S2** | VLAN 99 | 10.209.99.22 | 255.255.255.0 |
| **B1-S3** | VLAN 99 | 10.209.99.23 | 255.255.255.0 |

# 

# VLAN und Port Mappings

|  |  |  |  |
| --- | --- | --- | --- |
| **VLAN Number** | **Network Address** | **VLAN Name** | **Port Mappings** |
| **10** | 10.209.10.0/24 | Admin | F0/6 |
| **20** | 10.209.20.0/24 | Sales | F0/11 |
| **42** | 10.209.42.0/24 | Production | F0/16 |
| **99** | 10.209.99.0/24 | Mgmt&Native | F0/1-4 |
| **999** | N/A | BlackHole | Unused Ports |

# ACLs Problems

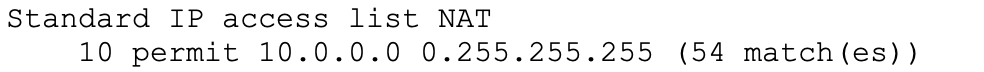
## The Specifications are impossible to accomplish

Text

Description automatically generated

## First change is also not doable

My second attempt was to split the ACL in two and do a second on the outgoing g0/1 Interface of the HQ Router to the Dater center. This also did not work out and after a lot of debugging and questioning of all my knowledge, I discovered that my matches for the NAT ACL are going up. That’s because every traffic that goes out to the Internet or the Datacenter gets translated. This means it is impossible to write an ACL with source addresses



# Final Solution for the ACL

The Problems are manly caused by the wrong appliance of the ACLs. If you want to restrict the access with source addresses you need an extended ACL. The first rule of using an extended ACL is to apply it as close to the source as possible. Therefore, controlling the access of end-devices in the v-lans it is highly recommended to apply the ACL in the B1 Router on the g0/0 subinterfaces (g0/0.10,20,30) controlling the incoming traffic.

Text

Description automatically generated

10 allows the any device to acces the datacenter via http (80)

20 allows only the production PC subnet to enter the datacenter via https (443)

30 denies any other access of any pc from the vlans to access the datacenter

40 permits everything else, so that the pcs can still go to the internet and the dns server

50 is normal for every whitelist

Verification of the ACLs will be further down.

# Verification

## Path with hop counts

Production PC –(tracert)-> [www.pka](http://www.pka) blocked by ACL A picture containing text, remote, black, electronics

Description automatically generated

Production PC –(http)-> [www.pka](http://www.pka) works

Graphical user interface, application

Description automatically generated

Production PC –(https)-> [www.pka](http://www.pka) works Graphical user interface, application

Description automatically generated

Production PC –(tracert)-> [www.cisco.pka](http://www.cisco.pka) worksText

Description automatically generated

Production PC –(http)-> [www.cisco.pka](http://www.cisco.pka)

Graphical user interface, text, application

Description automatically generated

Production PC –(https)-> [www.cisco.pka](http://www.cisco.pka) Graphical user interface, text, application, email

Description automatically generated

Production PC –(tracert)-> Intranet.pka

Text

Description automatically generated

Production PC –(http)-> Intranet.pka Graphical user interface, application

Description automatically generated

Production PC –(https)-> Intranet.pka workingGraphical user interface, application

Description automatically generated

Outside Host –(http)-> [www.pka](http://www.pka) working Graphical user interface, application

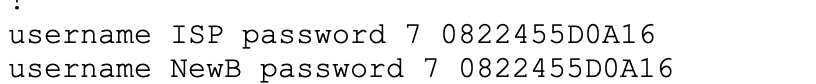
Description automatically generated

## DNS with command Line

Text

Description automatically generated with medium confidence

## PPP



Text

Description automatically generated

NewB-PC1 –(tracert)-> [www.pka](http://www.pka)

Text

Description automatically generated with medium confidence

## BGP



Text

Description automatically generated

Text

Description automatically generated

## Port Security

Table

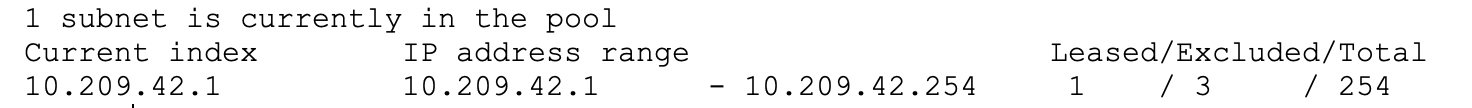
Description automatically generated

## DHCP

Table

Description automatically generated with low confidence

A picture containing diagram

Description automatically generated 

## VLANs

Table

Description automatically generated

Table

Description automatically generated

## Inter-VLAN routing

Text

Description automatically generated

## Dynamic, Static and default Routing

HQ

Text

Description automatically generated

B1

Text

Description automatically generated

## SSH Telnet

Telnet gets blocked, connections are only allowed with the SSH protocol:

Text

Description automatically generated

Two retries:

Text

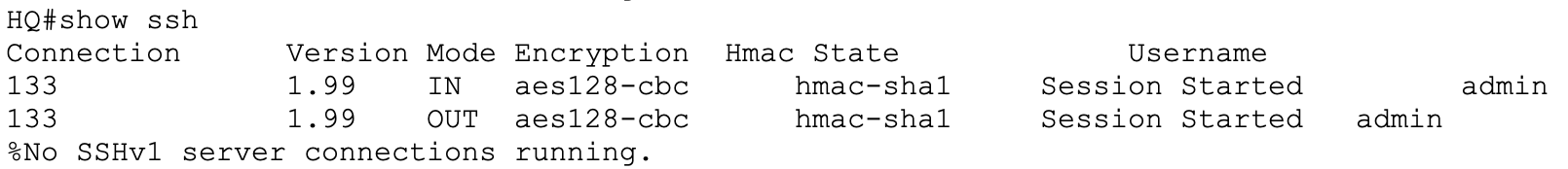
Description automatically generated

60 Second timeout:

Text

Description automatically generated

HQ connection:



## NAT

Text

Description automatically generated with low confidence

## ACL

Text

Description automatically generated

Text

Description automatically generated