1 Network diagram

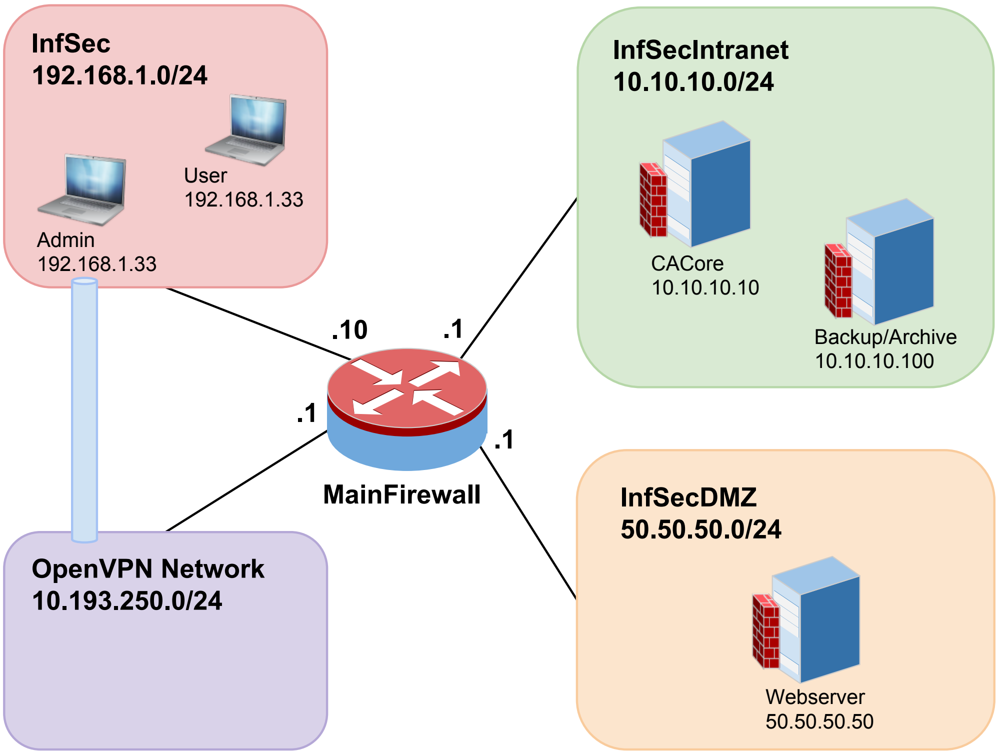

Figure 1: Network Diagram

2 Servers

All servers are equipped with at least one NIC corresponding to the network they are in as shown in Figure 1 and a NAT NIC that can be used for internet access (git, apt-get, etc.).

2.1 MainFirewall

Accounts & Passwords

admin: wT7nDB7A7d7V **root:** 5hmAMWxN6uVa

Installed software

IPCop

User for ssh access

Accesable only on 10.10.10.1 with port 8022 from 10.10.10.33 (user in InfSecIntranet) or from OpenVPN-Network.
ssh -p 8022 admin@10.10.10.1

Additional information

There is a webinterface on https://10.10.10.1:8023. Only accessable from 10.10.10.33 (user in InfSecIntranet).

2.2 Webserver

Accounts & Passwords

serveruser: 3FaVLt9RNxLu

operuser: KLs3PbjoXu9m

root: cLepMVRq8wDQ

operuser cannot use sudo/su and should therefore be used to run the application.

Installed software

Debian, iptables, nginx, python, flask, openSSL, openSSH

Running services (lsof -i)

sshd, nginx

User for ssh access

ssh {operuser, serveruser}@50.50.50.50

additional information

SSL signing key for HTTPS: 9klTRxBQcAnM

2.3 CoreCA

Accounts & Passwords

causer: 9BxkXM5fLLL8

operuser: PrCgs5TLqW4f

root: 8kSeddphG6Ac

operuser cannot use sudo/su and should therefore be used to run the application.

Installed software

Debian, iptables, python, mySQL, openSSL, openSSH

Running services (lsof -i)

sshd, mysql (only localhost)

User for ssh access

ssh {operuser, causer}@10.10.10.10

additional information

MySQL root: Cm7NsWBhf52C
MySQL dbuser: Q8mxLsBwTLJi
dbuser is only allowed to INSERT, SELECT, UPDATE the table user.iMovies, thus should be used for connecting to the database.

2.4 Backup/Archive Server

Accounts & Passwords

archiveuser: 4uMtrPMLxShw	**operuser:** QT5wbxjCN8gG
root: gaBWUt5EH8vU	

operuser cannot use sudo/su and should therefore be used to run the application.

Installed software

Debian, iptables, syslog, openSSH

Running services (lsof -i)

sshd

User for ssh access

ssh {operuser, archiveuser}@10.10.10.100

2.5 User

Accounts & Passwords

alice: alice

additional information

When running in netwok InfSec, VPN is possible (VPN start script on Desktop):

PKCS12 PW: StgmE58sadQu

When running in netwok InfSecIntranet, firewall web access on https://10.10.10.1:8023

3 Firewall rules

3.1 MainFirewall

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
Webserver	HTTPS (443)	InfSec
InfSec	HTTPS (443)	Webserver
10.10.10.33	IPCop HTTPS (8023)	MainFirewall
OpenVPN network	IPCop SSH (8022)	MainFirewall
10.10.10.33	IPCop SSH (8022)	MainFirewall
BackupServer	IPCop SSH (8022)	MainFirewall
OpenVPN network	SSH (22)	Backupserver
OpenVPN network	SSH (22)	CACore
OpenVPN network	SSH (22)	Webserver
Webserver	RPC (4444)	CACore
CACore	RPC (4444)	Webserver
Backupserver	SSH (22)	Webserver
Webserver	SSH (22)	CACore
CACore	SSH (22)	Webserver
Webserver	syslog (10514)	Backupserver

3.2 Webserver

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
Backupserver	SSH (22)	Webserver
OpenVPN network	SSH (22)	Webserver
InfSec	HTTPS (443)	Webserver
CACore	RPC (4444)	Webserver
Webserver	HTTPS (443)	
Webserver	RPC (4444)	
Webserver	syslog (10514)	Backupserver
CACore	SSH (22)	Webserver
Webserver	SSH (22)	

3.3 CoreCA

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
Backupserver	SSH (22)	CACore
OpenVPN network	SSH (22)	CACore
Webserver	RPC (4444)	CACore
CACore	RPC (4444)	Webserver
CACore	SSH (22)	Backupserver
CAcore	syslog (10514)	Backupserver
Webserver	SSH (22)	CACore
CACore	SSH (22)	Webserver

3.4 Backup/Archive Server

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
CACore	SSH (22)	Backupserver
OpenVPN network	SSH (22)	Backupserver
Backupserver	SSH (22)	CACore
Backupserver	SSH (22)	MainFirewall
Backupserver	SSH (22)	Webserver
Webserver	syslog (10514)	Backupserver
CAcore	syslog (10514)	Backupserver