

Lab 1

Author: Benjamin Medicke

Topics: Basics, SSH & VNC NAT

lab1 | lab2 | lab3 | lab4

- Lab 1.1 Connecting to Management
- Lab 1.2 SSH Connection to Linux Instance
 - 1.2.1 Subnet hinter NAT
 - 1.2.2 Neue Policies
 - 1.2.3 Management Traffic & Stealth-Rule
 - 1.2.4 Logging
 - 1.2.5 Install Policy
 - 1.2.6 Testen der SSH Keys
 - Aufgetretene Probleme
- Lab 1.3 VNCServer & NAT Rules
 - 1.3.1 Regel erstellen: Internetzugriff für die Linux Instanz
 - 1.3.2 Login und Internet-Test
 - 1.3.3 apt Installationen
 - 1.3.4 VNC Server starten
 - 1.3.5 Erstellen von Security Policies
 - 1.3.6 Testen der VNC Verbindung
 - 1.3.7 Aufgetretene Probleme

Lab 1.1 Connecting to Management

Der Fingerprint des Servers, der bei der ersten Verbindung angezeigt wird ist:

```
REAR NECK KICK TIP HOE DUET DALE GASH ECHO OW SHED TONE
```

Er stimmt mit dem im Gaia Web Interface überein.

Certificate Authority

Certificate Authority Status:	Established
Security Management DN:	o=cloudguard-gw-vm...u7rvfg
Fingerprint:	REAR NECK KICK TIP HOE DUET DALE GASH ECHO OW SHED TONE
<input type="button" value="Reset"/>	

Fingerprint im Gaia Web Interface

Beantworten Sie die Frage: Welche Aufgaben hat der Fingerprint und welche Bedrohungen werden damit verhindert?


Der Fingerprint garantiert die Authentizität des Servers. Falls der Server 'ausgetauscht' wird, können Man-In-The-Middle Angriffe erkannt werden. Wenn sich der Fingerprint geändert hat, deutet das auf eine Änderung des Private Keys des Servers hin. Dies kann darauf hinweisen, dass sich ein Angreifer als der Zielserver ausgibt. Es sollte sichergestellt werden, dass der Server integer ist.

Lab 1.2 SSH Connection to Linux Instance

1.2.1 Subnet hinter NAT

Anlegen eines neuen Netzwerkobjektes (Subnetz 192.168.20.0/24), welches mit NAT hinter der Firewall versteckt wird.

New Network

 **NAT**
Enter Object Comment

General
NAT

IPv4

Network address: 192.168.20.0

Net mask: 255.255.255.0

Broadcast address:


☒ Included
☐ Not included

IPv6

Network address:

Prefix:


Groups

 Add Tag

OK Cancel

Neues Netzwerkobjekt, Reiter: General

New Network

 **NAT**
Enter Object Comment

General
NAT

Values for address translation

☒ Add automatic address translation rules

Translation method: Hide


☒ Hide behind the gateway
☐ Hide behind IP address

IPv4 address: 0.0.0.0

IPv6 address: ::

Install on gateway: * All

Groups

 Add Tag

OK Cancel

Neues Netzwerkobjekt, Reiter: NAT.

Aktivieren von "Add automatic address translation rule", "Hide" und "Hide behind the gateway".

Ebenso wurde ein Host-Objekt angelegt, welches die Linux Instanz (IP:

192.168.20.50) abbildet.

The screenshot shows a 'Host' configuration window titled 'Linux Instance' with the subtitle 'Enter Object Comment'. On the left is a sidebar with tabs: 'General' (selected), 'Network Management', 'NAT', 'Advanced', 'Servers', and 'Groups'. The main area is titled 'Machine' and contains fields for 'IPv4 address' (192.168.20.50) and 'IPv6 address' (empty). A 'Resolve from name' button is next to the IPv4 field. At the bottom of the main area is an 'Add Tag' button. At the bottom of the window are 'OK' and 'Cancel' buttons.

Neues Netzwerkobjekt: Linux Instance

1.2.2 Neue Policies

Anlegen neuer Policies um SSH Zugriff auf Linux Instanz zu ermöglichen. Beachte:

Auf Port 22 läuft bereits der SSH Server der CloudGuard Instanz, daher wird hier Port 2222 verwendet. Die folgenden Regeln wurden erstellt:

1. eine Firewallregel, die Port 2222 (für SSH) auf die CloudGuard Instanz erlaubt
2. eine NAT-Regel, die Port 2222 der CloudGuard Instanz auf 22 der Linux Instanz mappt

The screenshot shows the 'New TCP Service' dialog box with the title 'SSH access' and a subtitle 'Enter Object Comment'. The 'General' tab is selected. The 'Protocol' is set to 'SSH2'. A description states: 'SSH is a network protocol and a tool for secure remote login over insecure networks. It provides an encrypted terminal session with strong authentication of both the server and client, using public-key cryptography.' Under 'Match By', 'Port' is set to 'Customize' with the value '2222'. A warning icon indicates 'Match for 'Any' Disabled.' and another warning icon indicates 'Protocol Signature is disabled'. At the bottom, there is an 'Add Tag' button and 'OK' and 'Cancel' buttons.

Neues TCP-Service-Object: SSH-access

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Linux: SSH custom port	* Any	cloudguard-gw-vm	* Any	SSH_on_2222	Accept
2	Cleanup rule	* Any	* Any	* Any	* Any	Drop

Firewallregel, die Port 2222 erlaubt.

Manual Lower Rules (5)							
5	* Any	cloudguard-gw-vm	SSH_on_2222	Original	Linux Instance	ssh_version_2	* Policy Targets

NAT Regel.

1.2.3 Management Traffic & Stealth-Rule

Hier werden zwei weitere Regeln erstellt:

1. Erlauben von Management-Traffic
2. Stealth Regel (restlichen Traffic dropen)

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Linux: SSH custom port	* Any	cloudguard-gw-vm	* Any	SSH_on_2222	Accept	Log	* Policy Targets
2	Cloudguard: management	* Any	cloudguard-gw-vm	* Any	ssh_version_2 https FW1_ica_mgmt_tools FW1_mgmt	Accept	Log	* Policy Targets
3	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

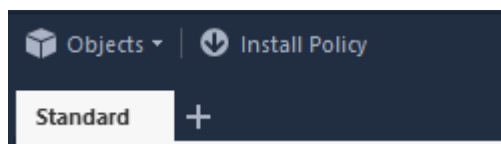
Neue Management und Stealth Regeln

1.2.4 Logging

Jetzt wurde Logging für alle Regeln aktiviert (siehe vorherigen Screenshot).

1.2.5 Install Policy

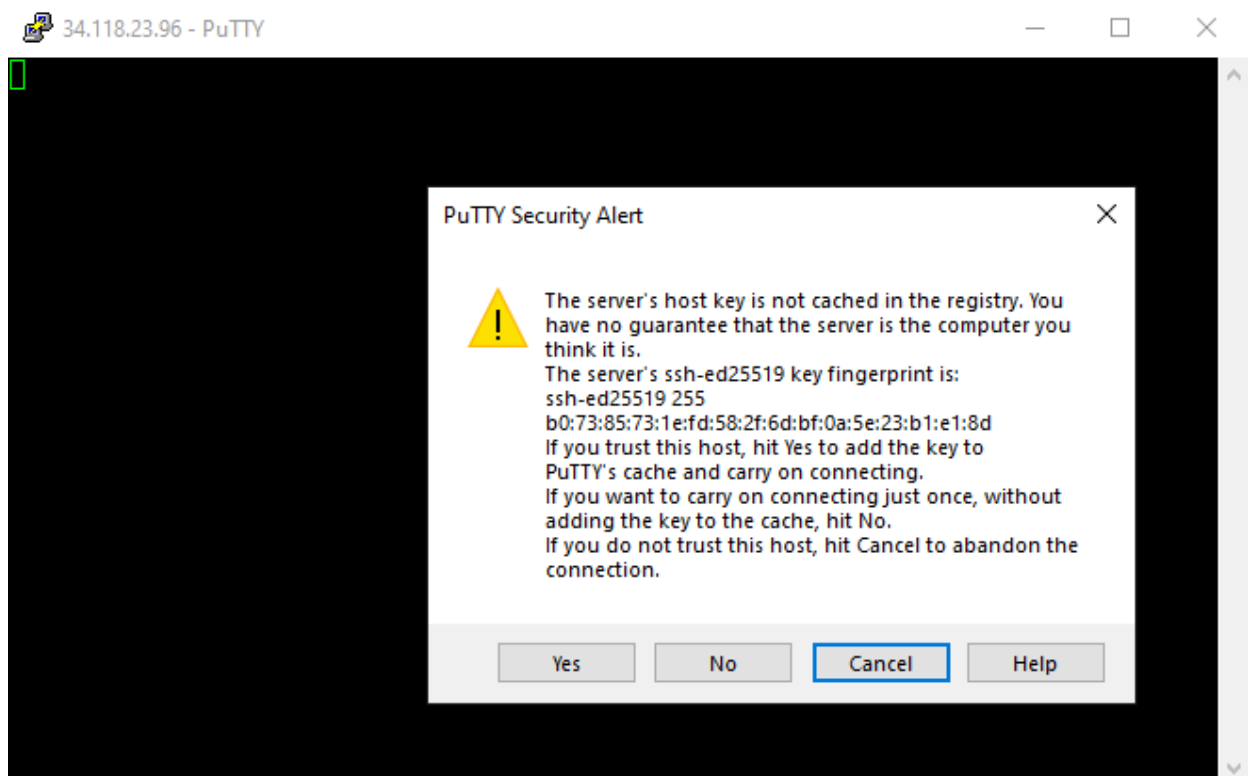
Die Policies wurden mit "Install Policy" installiert.



Install Policy Button

1.2.6 Testen der SSH Keys

Abschließend wurde die Verbindung getestet.



Bei der initialen Verbindung wird der SSH key angezeigt. Dieser sollte verglichen und akzeptiert werden.

```

cs20m027@linux-vm: ~
login as: cs20m027
Authenticating with public key "cs20m027"
Linux linux-vm 4.19.0-16-cloud-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 28 18:00:44 2021 from 35.235.241.240
cs20m027@linux-vm:~$ whoami
-bash: whoami: command not found
cs20m027@linux-vm:~$ whoami
cs20m027
cs20m027@linux-vm:~$ █

```

Erfolgreicher Login via SSH Key auf die Linux Instanz

```

admin@cloudguard-gw-vm:~
Using username "admin".
Pre-authentication banner message from server:
| This system is for authorized use only.
End of banner message from server
Authenticating with public key "admin"
You have logged into the system.
By using this product you agree to the terms and conditions
as specified in https://www.checkpoint.com/download_agreement.html
This product uses open source software as specified in
/opt/opensource/README.
[Expert@cloudguard-gw-vm:0]# █

```

Erfolgreicher Login via SSH Key auf die CloudGuard Instanz

Aufgetretene Probleme

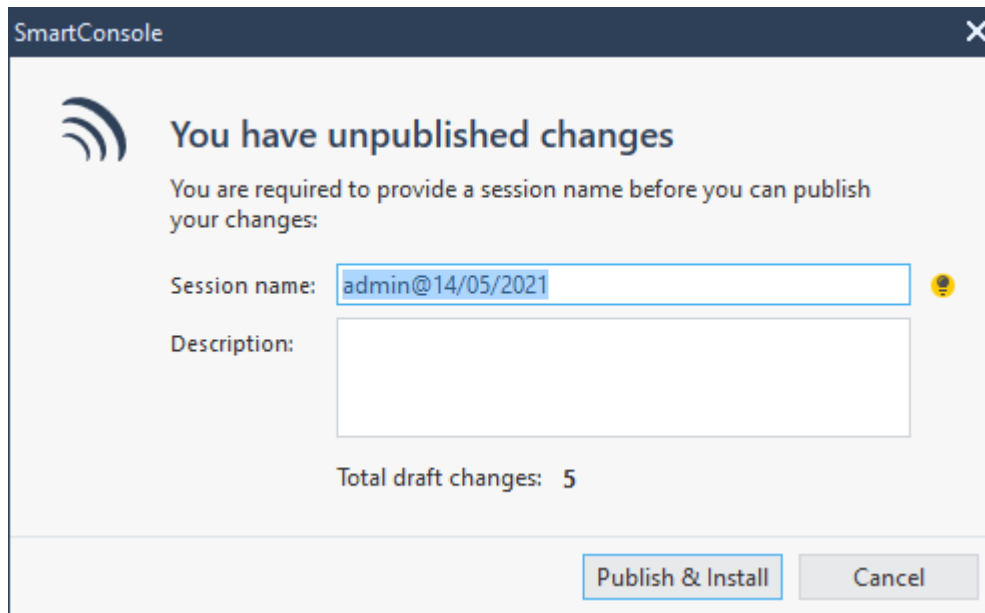
Es sind keine Probleme aufgetreten.

Lab 1.3 VNCServer & NAT Rules

1.3.1 Regel erstellen: Internetzugriff für die Linux Instanz

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Linux Internet access	Linux Instance	* Any	* Any	* Any	Accept	Log	* Policy Targets

Policy, die Internetzugriff für die Linux Instanz erlaubt



Publish & Install

1.3.2 Login und Internet-Test

Diese neue Regel wurde mit `ping` erfolgreich getestet.

```
cs20m027@linux-vm: ~  
cs20m027@linux-vm:~$ ping 1.1.1.1  
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.  
64 bytes from 1.1.1.1: icmp_seq=10 ttl=54 time=3.41 ms  
64 bytes from 1.1.1.1: icmp_seq=11 ttl=54 time=2.96 ms  
64 bytes from 1.1.1.1: icmp_seq=12 ttl=54 time=11.3 ms  
64 bytes from 1.1.1.1: icmp_seq=13 ttl=54 time=2.68 ms  
64 bytes from 1.1.1.1: icmp_seq=14 ttl=55 time=2.73 ms  
64 bytes from 1.1.1.1: icmp_seq=15 ttl=55 time=2.95 ms  
64 bytes from 1.1.1.1: icmp_seq=16 ttl=55 time=2.23 ms  
64 bytes from 1.1.1.1: icmp_seq=17 ttl=54 time=2.63 ms  
64 bytes from 1.1.1.1: icmp_seq=18 ttl=54 time=8.79 ms  
64 bytes from 1.1.1.1: icmp_seq=19 ttl=54 time=3.27 ms  
64 bytes from 1.1.1.1: icmp_seq=20 ttl=54 time=2.82 ms  
64 bytes from 1.1.1.1: icmp_seq=21 ttl=54 time=2.59 ms  
^C  
--- 1.1.1.1 ping statistics ---  
21 packets transmitted, 12 received, 42.8571% packet loss, time 233ms  
rtt min/avg/max/mdev = 2.227/4.031/11.328/2.761 ms  
cs20m027@linux-vm:~$
```

Der Ping geht durch!

1.3.3 apt Installationen

In den nächsten Schritten wurden zusätzliche Pakete installiert:

- `xfce4`
- `xfce4-goodies`
- `tightvncserver`


```
cs20m027@linux-vm: ~  
Get:36 http://deb.debian.org/debian buster-backports/main amd64 Packages 2021-05  
-04-2002.50.pdiff [1095 B]  
Get:37 http://deb.debian.org/debian buster-backports/main amd64 Packages 2021-05  
-05-0201.29.pdiff [889 B]  
Get:38 http://deb.debian.org/debian buster-backports/main amd64 Packages 2021-05  
-10-0200.35.pdiff [175 B]  
Get:39 http://deb.debian.org/debian buster-backports/main amd64 Packages 2021-05  
-11-1400.52.pdiff [679 B]  
Get:39 http://deb.debian.org/debian buster-backports/main amd64 Packages 2021-05  
-11-1400.52.pdiff [679 B]  
Get:40 http://deb.debian.org/debian buster-backports/main Translation-en 2021-05  
-11-1400.52.pdiff [243 B]  
Get:41 http://packages.cloud.google.com/apt google-cloud-packages-archive-keyring-  
buster/main amd64 Packages [396 B]  
Get:40 http://deb.debian.org/debian buster-backports/main Translation-en 2021-05  
-11-1400.52.pdiff [243 B]  
Get:42 http://packages.cloud.google.com/apt google-compute-engine-buster-stable/  
main amd64 Packages [1784 B]  
Fetched 1096 kB in 1s (962 kB/s)  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
10 packages can be upgraded. Run 'apt list --upgradable' to see them.  
cs20m027@linux-vm:~$
```

```
sudo apt update
```

```
cs20m027@linux-vm: ~  
x11-xkb-utils x11-xserver-utils xarchiver xauth xbitmaps xdg-user-dirs  
xdg-utils xfburn xfce4 xfce4-appfinder xfce4-battery-plugin xfce4-clipman  
xfce4-clipman-plugin xfce4-cpufreq-plugin xfce4-cpugraph-plugin  
xfce4-datetime-plugin xfce4-dict xfce4-diskperf-plugin xfce4-fsguard-plugin  
xfce4-genmon-plugin xfce4-goodies xfce4-mailwatch-plugin  
xfce4-netload-plugin xfce4-notes xfce4-notes-plugin xfce4-notifyd  
xfce4-panel xfce4-places-plugin xfce4-power-manager xfce4-power-manager-data  
xfce4-power-manager-plugins xfce4-pulseaudio-plugin xfce4-screenshooter  
xfce4-sensors-plugin xfce4-session xfce4-settings xfce4-smartbookmark-plugin  
xfce4-systemload-plugin xfce4-taskmanager xfce4-terminal xfce4-timer-plugin  
xfce4-verve-plugin xfce4-wavelan-plugin xfce4-weather-plugin  
xfce4-whiskermenu-plugin xfce4-xkb-plugin xfconf xfdesktop4 xfdesktop4-data  
xfonts-100dpi xfonts-75dpi xfonts-base xfonts-encodings xfonts-scalable  
xfonts-utils xfwm4 xinit xkb-data xorg xorg-docs-core xserver-common  
xserver-xorg xserver-xorg-core xserver-xorg-input-all  
xserver-xorg-input-libinput xserver-xorg-input-wacom xserver-xorg-legacy  
xserver-xorg-video-all xserver-xorg-video-amdgpu xserver-xorg-video-ati  
xserver-xorg-video-fbdev xserver-xorg-video-intel xserver-xorg-video-nouveau  
xserver-xorg-video-qxl xserver-xorg-video-radeon xserver-xorg-video-vesa  
xserver-xorg-video-vmware xterm  
0 upgraded, 492 newly installed, 0 to remove and 10 not upgraded.  
Need to get 197 MB of archives.  
After this operation, 859 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

```
sudo apt install xfce4 xfce4-goodies
```

```

cs20m027@linux-vm: ~
Setting up libvorbisfile3:amd64 (1.3.6-2) ...
Setting up perl (5.28.1-6+deb10u1) ...
Setting up xfonts-base (1:1.0.5) ...
Setting up libsecret-1-0:amd64 (0.18.7-1) ...
Setting up libdata-dump-perl (1.23-1) ...
Setting up libxfixes3:amd64 (1:5.0.3-1) ...
Setting up libipc-system-simple-perl (1.25-4) ...
Setting up libxml-xpathengine-perl (0.14-1) ...
Setting up shared-mime-info (1.10-1) ...
Setting up libxinerama1:amd64 (2:1.1.4-2) ...
Setting up libxv1:amd64 (2:1.0.11-1) ...
Setting up libio-html-perl (1.001-1) ...
Setting up libxrandr2:amd64 (2:1.5.1-1) ...
Setting up libcroco3:amd64 (0.6.12-3) ...
Setting up gvfs-libs:amd64 (1.38.1-5) ...
Setting up libblockdev-fs2:amd64 (2.20-7+deb10u1) ...
Setting up aspell (0.60.7~20110707-6) ...
Setting up usbmuxd (1.1.1~git20181007.f838cf6-1) ...
Warning: The home dir /var/lib/usbmux you specified can't be accessed: No such file or directory
Adding system user `usbmux' (UID 107) ...
Adding new user `usbmux' (UID 107) with group `plugdev' ...
Progress: [ 73%] [#####.....]

```

Was eine Weile dauert.

```

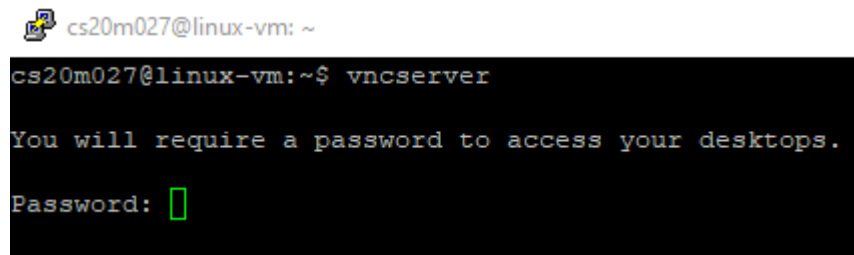
cs20m027@linux-vm: ~
tightvnc-java
The following NEW packages will be installed:
tightvncserver
0 upgraded, 1 newly installed, 0 to remove and 10 not upgraded.
Need to get 689 kB of archives.
After this operation, 1857 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 tightvncserver amd64 1:1.3.9-9+deb10u1 [689 kB]
Fetched 689 kB in 0s (4800 kB/s)
Selecting previously unselected package tightvncserver.
(Reading database ... 74891 files and directories currently installed.)
Preparing to unpack .../tightvncserver_1%3a1.3.9-9+deb10u1_amd64.deb ...
Unpacking tightvncserver (1:1.3.9-9+deb10u1) ...
Setting up tightvncserver (1:1.3.9-9+deb10u1) ...
update-alternatives: using /usr/bin/tightvncserver to provide /usr/bin/vncserver (vncserver) in auto mode
update-alternatives: using /usr/bin/Xtightvnc to provide /usr/bin/Xvnc (Xvnc) in auto mode
update-alternatives: using /usr/bin/tightvncpasswd to provide /usr/bin/vncpasswd (vncpasswd) in auto mode
Processing triggers for man-db (2.8.5-2) ...
cs20m027@linux-vm:~$

```

```
sudo apt install tightvncserver
```

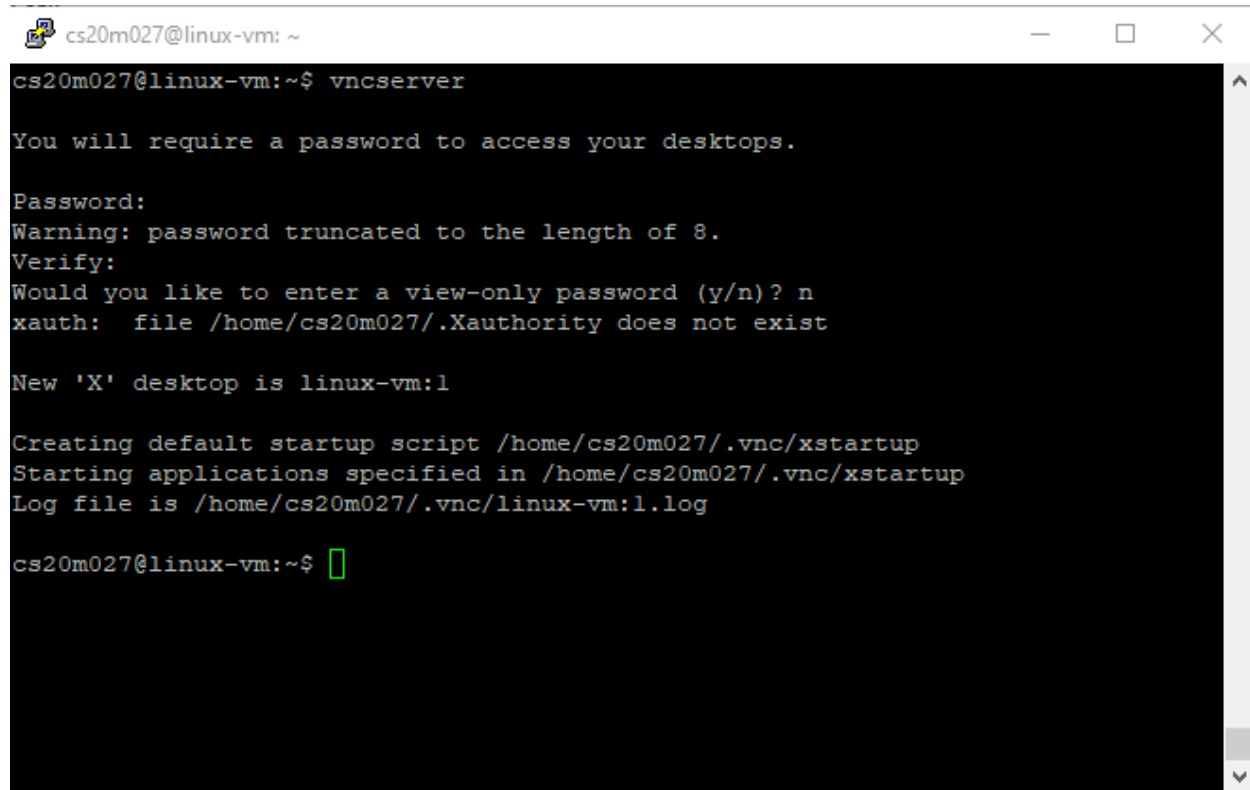
1.3.4 VNC Server starten

Daraufhin wurde der VNC Server gestartet und konfiguriert. Ebenso wurde die installierte Desktop-Umgebung aktiviert und ein `systemd` Unit-File für den VNC Server eingerichtet und gestartet.



```
cs20m027@linux-vm: ~  
cs20m027@linux-vm:~$ vncserver  
You will require a password to access your desktops.  
Password: [ ]
```

Passwortvergabe für den VNC Service



```
cs20m027@linux-vm: ~  
cs20m027@linux-vm:~$ vncserver  
You will require a password to access your desktops.  
Password:  
Warning: password truncated to the length of 8.  
Verify:  
Would you like to enter a view-only password (y/n)? n  
xauth:  file /home/cs20m027/.Xauthority does not exist  
  
New 'X' desktop is linux-vm:1  
  
Creating default startup script /home/cs20m027/.vnc/xstartup  
Starting applications specified in /home/cs20m027/.vnc/xstartup  
Log file is /home/cs20m027/.vnc/linux-vm:1.log  
  
cs20m027@linux-vm:~$ [ ]
```

Gekürzte Passwörter wirken nicht sehr vertrauenserweckend...

```
cs20m027@linux-vm: ~  
#!/bin/sh  
  
xrdb $HOME/.Xresources  
startxfce4 &  
xsetroot -solid grey  
#x-terminal-emulator -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &  
#x-window-manager &  
# Fix to make GNOME work  
export XKL_XMODMAP_DISABLE=1  
/etc/X11/Xsession  
~  
~  
~  
~  
~  
~  
:wq
```

Desktop-Umgebung (xfce4) Eintrag

```
cs20m027@linux-vm: ~  
cs20m027@linux-vm:~$ vim ~/.vnc/xstartup  
cs20m027@linux-vm:~$ sudo chmod +x ~/.vnc/xstartup  
cs20m027@linux-vm:~$
```

Ausführbar machen des Scripts.

```
cs20m027@linux-vm: ~  
cs20m027@linux-vm:~$ sudo vim /etc/systemd/system/vncserver@.service
```

Neuen Service anlegen

```
cs20m027@linux-vm: ~  
[Unit]  
Description=Start TightVNC server at startup  
After=syslog.target network.target  
  
[Service]  
Type=forking  
User=cs20m027  
Group=cs20m027  
WorkingDirectory=/home/cs20m027  
  
PIDFile=/home/cs20m027/.vnc/%H:%i.pid  
ExecStartPre=-/usr/bin/vncserver -kill :%i > /dev/null 2>&1  
ExecStart=/usr/bin/vncserver -depth 24 -geometry 1280x800 :%i  
ExecStop=/usr/bin/vncserver -kill :%i  
  
[Install]  
WantedBy=multi-user.target  
~  
17,27 All
```

Editiertes Service Script

```
cs20m027@linux-vm: ~
cs20m027@linux-vm:~$ sudo systemctl daemon-reload
cs20m027@linux-vm:~$ sudo systemctl enable vncserver@1.service
Created symlink /etc/systemd/system/multi-user.target.wants/vncserver@1.service
→ /etc/systemd/system/vncserver@.service.
cs20m027@linux-vm:~$ sudo systemctl start vncserver@1
cs20m027@linux-vm:~$
```

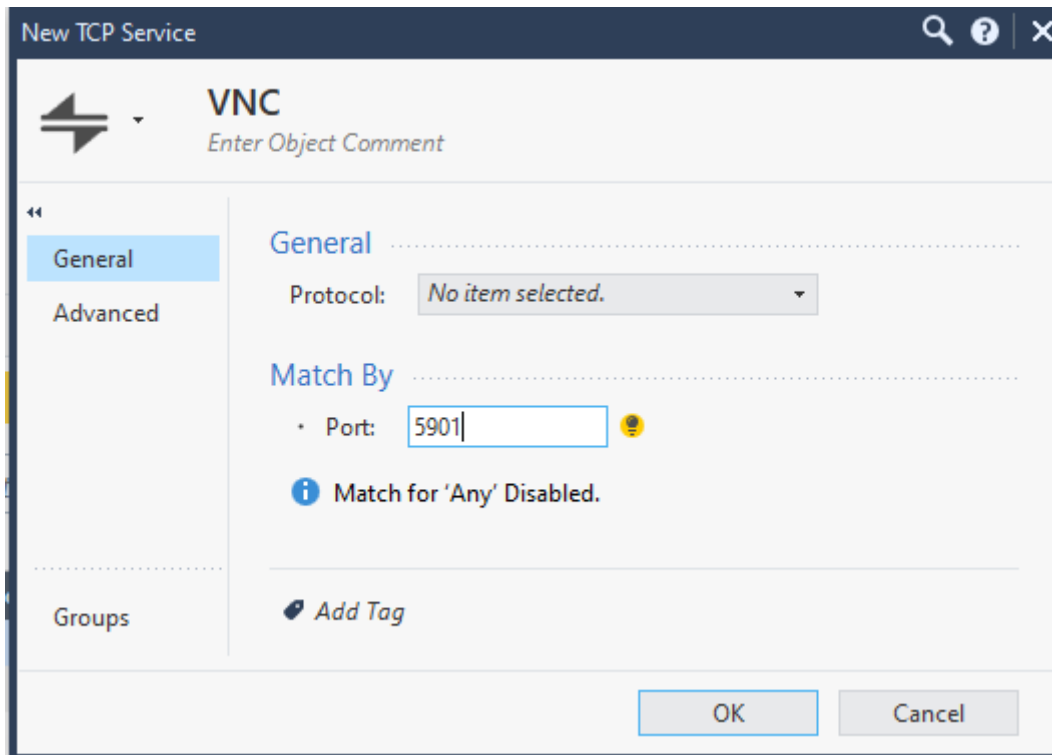
Regenerieren des Dependency-Trees, VNC Service Autostart aktivieren und starten

```
cs20m027@linux-vm: ~
● vncserver@1.service - Start TightVNC server at startup
   Loaded: loaded (/etc/systemd/system/vncserver@.service; enabled; vendor preset: enab
   Active: active (running) since Fri 2021-05-14 15:48:31 UTC; 3min 16s ago
   Process: 14236 ExecStartPre=/usr/bin/vncserver -kill :1 > /dev/null 2>&1 (code=exited
   Process: 14240 ExecStart=/usr/bin/vncserver -depth 24 -geometry 1280x800 :1 (code=exi
   Main PID: 14248 (Xtightvnc)
      Tasks: 88 (limit: 4665)
     Memory: 108.4M
    CGroup: /system.slice/system-vncserver.slice/vncserver@1.service
           └─14248 Xtightvnc :1 -desktop X -auth /home/cs20m027/.Xauthority -geometry 1
              └─14252 /bin/sh /home/cs20m027/.vnc/xstartup
                 └─14254 /bin/sh /etc/xdg/xfce4/xinitrc -- /etc/X11/xinit/xserverrc
                    └─14257 /bin/sh /etc/xdg/xfce4/xinitrc -- /etc/X11/xinit/xserverrc
                       └─14275 dbus-launch --autolaunch eb7539ffca1990blb7da44670bc9lada --binary-s
                          └─14277 xfce4-session
                             └─14278 /usr/bin/dbus-daemon --syslog-only --fork --print-pid 5 --print-addr
                                └─14288 /usr/bin/dbus-launch --sh-syntax --exit-with-session xfce4-session
                                   └─14290 /usr/bin/dbus-daemon --syslog --fork --print-pid 5 --print-address 7
                                      └─14299 /usr/bin/dbus-launch --exit-with-session --sh-syntax
                                         └─14300 /usr/bin/dbus-daemon --syslog --fork --print-pid 5 --print-address 7
                                            └─14311 /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
lines 1-21
```

Der Service läuft!

1.3.5 Erstellen von Security Policies

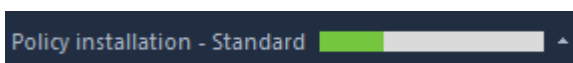
Um den Zugriff auf die Linux Instanz über VNC zu ermöglichen wurden die folgenden Security Policies erstellt:



Neues VNC Service Objekt auf Port 5901

Manual Lower Rules (5-6)								
5	* Any	cloudguard-gw-	VNC	= Original	Linux Instance	VNC	* Policy Targets	
6	* Any	cloudguard-gw-	SSH_on_2222	= Original	Linux Instance	ssh_version_2	* Policy Targets	

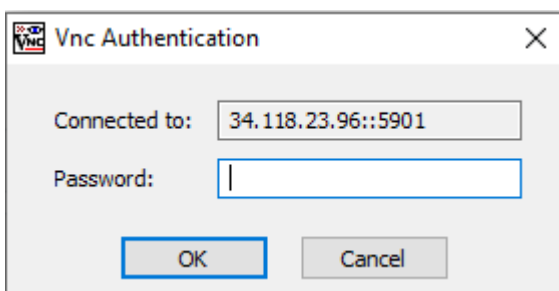
NAT für den VNC Service (von CloudGuard auf Linux Instanz, jeweils Port 5901)



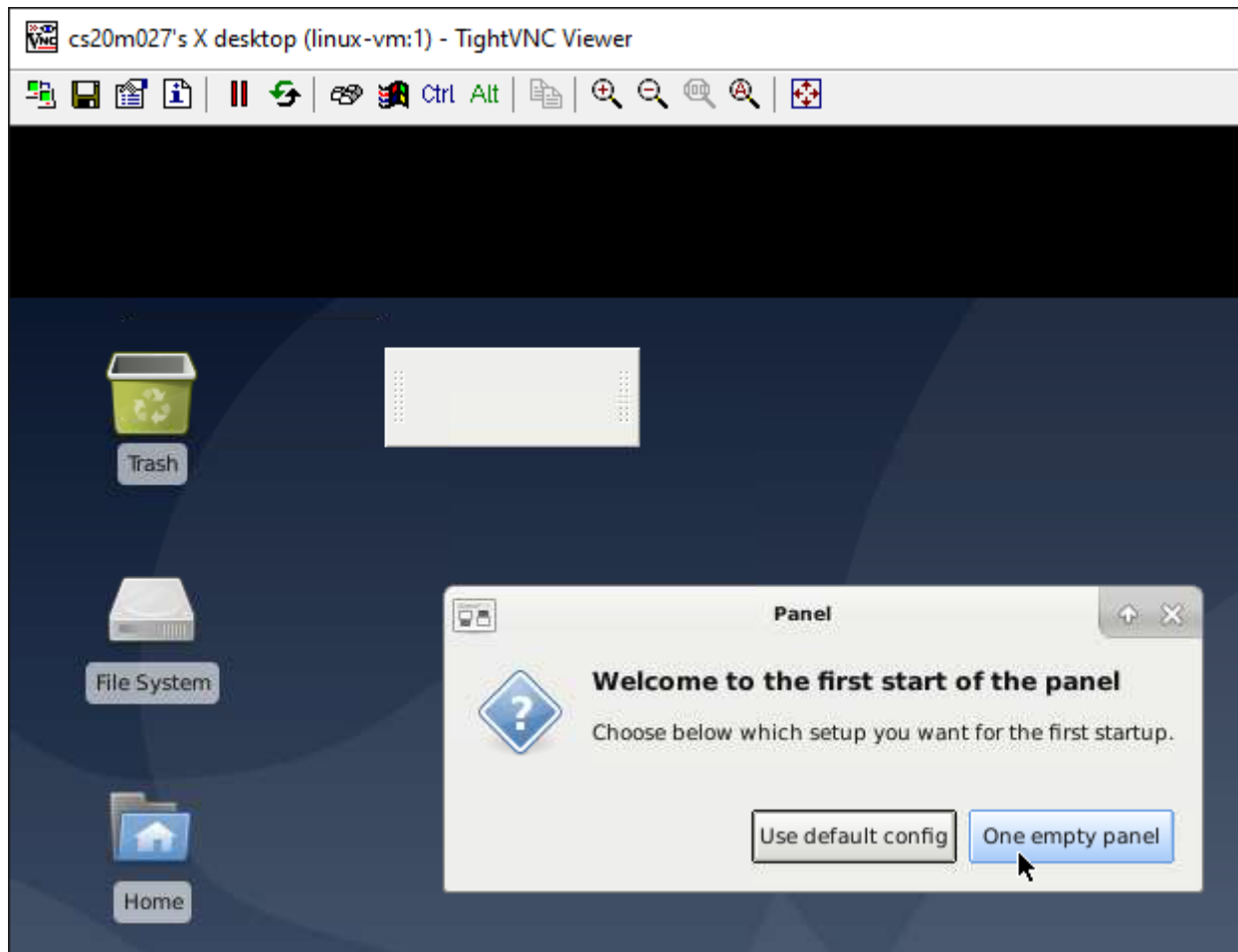
Installieren der Policy

1.3.6 Testen der VNC Verbindung

Im letzten Schritt wurde die Verbindung mit dem TightVNC Viewer erfolgreich getestet.



Der VNC Verbindungsaufbau funktioniert



Der VNC Login war erfolgreich

1.3.7 Aufgetretene Probleme

- Der automatische Vollbildmodus hatte leichte Grafikfehler
- gelöst durch `Strg-Alt-Shift-F` um den Modus zu verlassen

nächstes Lab