

Firewall-Regel hinzufügen (Port 25)

Zuhause nutze ich nur die kostenlose Version des ESXi, auf ein Backup meiner virtuellen Maschinen möchte ich aber doch nicht verzichten. Da die freie ESXi-Version leider nur lesenden API-Zugriff hat, kommen die ganzen schönen Backup-Tools wie Veam oder HPE VM Explorer leider nicht in Frage, da diese mit der Data Protection API arbeiten.

So setze ich dann das wohl allseits bekannte Skript ghettoVCB ein, was auch prima funktioniert, allerdings scheitert der abschließende EMail-Versand, da die ESXi-Firewall den Port 25 ausgehend sperrt. Wer nun versucht den Port in der Firewall zu öffnen, wird verwundert feststellen, dass dafür gar keine Firewall-Regel existiert.

Zum Glück ist es relativ einfach möglich eigene Firewall-Regeln zu definieren.

Zunächst mal per SSH auf den ESXi-Host einloggen.

Die Firewall-Regeln werden in XML-Dateien im Verzeichnis `/etc/vmware/firewall` definiert.

1. Eine Datei namens `SMTP.xml` in diesem Verzeichnis anlegen

```
vi /etc/vmware/firewall/sntp.xml
```

2. Und diesen Inhalt einfügen.

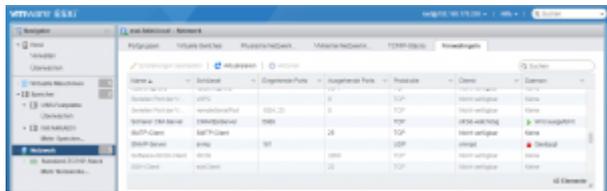
```
1 <ConfigRoot>
2 <service id='1010'>
3 <id>SMTP-Client</id>
4 <rule id='0000'>
5 <direction>outbound</direction>
6 <protocol>tcp</protocol>
7 <porttype>dst</porttype>
8 <port>25</port>
9 </rule>
10 <enabled>true</enabled>
11 <required>false</required>
12 </service>
13 </ConfigRoot>
```

Wichtig hierbei ist, dass man eine eindeutige service id verwendet, bei meiner ESXi-Versionen gehen diese als Standard bis 43, so dass die hier verwendete 1010 wohl ausreichenden Sicherheitsabstand hat.

3. Die Firewall-Regeln neu einlesen

```
esxcli network firewall refresh
```

4. Und da ist sie auch schon und der Email-Versand funktioniert nun wie gewünscht.



SMTP-Client in den Firewallregeln

5. Leider ist unsere soeben angelegte xml-Datei nach einem Reboot wieder verschwunden, wir müssen also einen Weg finden, dass die Firewall-Regel auch einen Neustart des ESXi-Hosts überlebt. Auch hier gibt es glücklicherweise eine relativ einfache Lösung.

6. Wir kopieren unsere gerade erstellte XML-Datei auf einen im System angelegten Datatstore, da sich dort befindliche Dateien auch einen Neustart überleben. Auf meinem ESXi-Host ist das z.B. eine USB-Festplatte, die zur Datensicherung genutzt wird.

```
cp /etc/vmware/firewall/smtp.xml /vmfs/volumes/USB-Festplatte/configs/
```

7. Nun müssen wir nur noch dafür sorgen, dass die so gesicherte Datei bei einem Neustart auch wieder an den angestammten Ort zurück kopiert wird. Hierzu bedienen wir uns des Scripts /etc/rc.local.d/local.sh, welches bei jedem Start ausgeführt wird. Wir fügen folgende Zeilen hinzu:

```
1 /bin/cp /vmfs/volumes/USB-Festplatte/configs/smtp.xml /etc/vmware/firewall
2 /bin/esxcli network firewall refresh
```

8. So, damit ist die Firewall-Regel nun persistent und überlebt auch einen Reboot des ESXi-Servers.

Permanent link:

<http://wiki.richter-ch.de/doku.php/wiki:computer:esxi:port25>

Last update: **2022/02/07 15:55**

