invisAD-setup - action #54860

Firewall: NAT Rules for inbound Routing via VPN are missing.

2019-07-30 12:28 - flacco

Status:	Closed	**Start date:**	2019-07-30
Priority:	Normal	**Due date:**	2020-06-01
Assignee:	flacco	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	14.2		

Description

It seems to be impossible to reach hosts inside the internal net via OpenVPN Connections.

To set them manually the following commands are necessary:

```
firewall-cmd --direct --permanent --add-rule ipv4 nat POSTROUTING 0 -o intern -j MASQUERADE
firewall-cmd --direct --permanent --add-rule ipv4 filter FORWARD 0 -i vpn -o intern -j ACCEPT
firewall-cmd --direct --permanent --add-rule ipv4 filter FORWARD 0 -i intern -o vpn -m state --sta
te RELATED,ESTABLISHED -j ACCEPT
```

Untestet yet.

History

#1 - 2019-07-30 13:08 - EDV_Lotse

Ich habe gerade getestet: es funktioniert.
Die Befehle haben eine Datei /etc/firewalld/direct.xml erzeugt.
Kann man das Gleiche über Konfigurationsdateien erreichen?

#2 - 2019-07-30 13:27 - flacco

- Status changed from New to In Progress

- % Done changed from 0 to 20

Das war der Plan. Kannst Du die Datei mal hier ans Ticket anhängen?

#3 - 2019-07-30 14:12 - EDV_Lotse

- File direct.xml added

- Status changed from In Progress to Workable

- % Done changed from 20 to 0

#4 - 2019-07-30 14:17 - flacco

- Status changed from Workable to In Progress

- % Done changed from 0 to 20

#5 - 2019-07-30 17:41 - flacco

- Status changed from In Progress to Feedback

Ja, die Datei können wir einfach ins Setup integrieren. Ich bin nur am überlegen, ob wir das pauschal im sine2 Modul firewall machen oder im Modul openvpn. Früher war openvpn mal ein optionales Modul, es hätte also Sinn gemacht, die Firewall Erweiterung nur dann einzurichten, wenn openVPN au genutzt wird.

Aktuell ist openvpn nicht optional, also wäre der erste Weg auch ok.

Was denkt Ihr?

#6 - 2019-07-31 18:06 - ingogoeppert

vpn steht in der Liste der internen Devices. Mir ist nicht klar warum man da überhaupt extra Regeln dafür braucht. Sollte zwischen den internen nicht eh alles erlaubt sein? Woher kommen die Befehle?

#7 - 2019-08-02 15:54 - flacco

- % Done changed from 20 to 30

Das hatten wir im alten SUSEfirewall2 Setup auch drin, nannte sich "Classrouting", also NAT zwischen zwei internen Devices.

Die Befehle hab ich mit Googles Hilfe gefunden. Ich hatte das gleiche Problem wie Dimitri allerdings nicht auf einem invis-Server.

#8 - 2019-08-11 14:07 - ingogoeppert

- Target version changed from 14.1 to 14.2

#9 - 2019-08-26 08:00 - flacco

Ich habe mal die alten Konfigurationen aus unserem SuSEfirewall2 Setup herausgesucht:

-> Wir haben die VPN-Netzwerkschnittstelle der internen Zone zugeordnet:
FW_DEV_INT="intern vpn"

-> Wir haben für das VPN-Netz Masquerading aktiviert
FW_MASQ_NETS="192.168.166.0/24"

-> Wir hatten Classrouting für die interne Zone aktiviert:
FW_ALLOW_CLASS_ROUTING="int"

Das dürfte in etwa auf das heraus laufen, was ich mit den oben genannten zusätzlichen Regeln für den firewalld erreiche.

#10 - 2020-05-25 06:22 - flacco

- Due date set to 2020-06-01

#11 - 2020-05-25 14:30 - flacco

Wir sollten mal mit folgenden Regeln testen:

<?xml version="1.0" encoding="utf-8"?>
<direct>
<rule ipv="ipv4" table="filter" chain="FORWARD" priority="0">-i vpn -o intern -j ACCEPT</rule>
<rule ipv="ipv4" table="filter" chain="FORWARD" priority="0">-i intern -o vpn -j ACCEPT</rule>
</direct>

Mit dem ersten Satz könnte es Probleme NFS-Zugriffen geben.

#12 - 2020-05-25 14:30 - flacco

- % Done changed from 30 to 40

#13 - 2020-05-30 11:32 - flacco

- % Done changed from 40 to 60

direct.xml added to invis-setup

#14 - 2020-05-30 12:45 - flacco

- Status changed from Feedback to Closed

- % Done changed from 60 to 100

testet!

Done

Files

direct.xml	384 Bytes	2019-07-30	EDV_Lotse