FortiGate Bogon Block

Autoren: Morris Tichy, Lukas Freudensprung

Inhaltsverzeichnis

1. Theorie

Bogon sind private Adressen, die im öffentlichen Netz geblockt werden sollen. Auf der FortiGate werden daher eine local-in-policy erstellt die dazu dienen diese Adressen zu blockieren. Folgender Code blockiert diese Adressen.

2. Konfiguration

```bash
config firewall address
    edit "Bogon_0.0.0.0/8"
        set subnet 0.0.0.0 255.0.0.0
    next
    edit "Bogon_10.0.0.0/8"
        set subnet 10.0.0.0 255.0.0.0
    next
    edit "Bogon_100.64.0.0/10"
        set subnet 100.64.0.0 255.192.0.0
    next
    edit "Bogon_127.0.0.0/8"
        set subnet 127.0.0.0 255.0.0.0
    next
    edit "Bogon_169.254.0.0/16"
        set subnet 169.254.0.0 255.255.0.0
    next
    edit "Bogon_172.16.0.0/12"
        set subnet 172.16.0.0 255.240.0.0
    next
    edit "Bogon_192.0.0.0/24"
        set subnet 192.0.0.0 255.255.255.0
    next
    edit "Bogon_192.0.2.0/24"
        set subnet 192.0.2.0 255.255.255.0
    next
    edit "Bogon_192.168.0.0/16"
        set subnet 192.168.0.0 255.255.0.0
    next
    edit "Bogon_198.18.0.0/15"
        set subnet 198.18.0.0 255.254.0.0
    next
```

```
32      edit "Bogon_198.51.100.0/24"
33          set subnet 198.51.100.0 255.255.255.0
34      next
35      edit "Bogon_203.0.113.0/24"
36          set subnet 203.0.113.0 255.255.255.0
37      next
38      edit "Bogon_224.0.0.0/4"
39          set subnet 224.0.0.0 240.0.0.0
40      next
41      edit "Bogon_240.0.0.0/4"
42          set subnet 240.0.0.0 240.0.0.0
43      next
44      edit "Bogon_255.255.255.255/32"
45  set subnet 255.255.255.255 255.255.255.255
46      next
47  end
```

```bash
1  Dieser Codeabschnitt legt die Adressen die später blockiert werden sollen fest
2
3  config firewall addrgrp
4      edit "Bogon_Addresses"
5          set member "Bogon_0.0.0.0/8" "Bogon_10.0.0.0/8" "Bogon_100.64.0.0/10" "Bogon_127.0.0.0/8" "Bogon_169.254.0.0/16" "Bogon_172.16.0.0/12" "Bogon_192.0.0.0/24" "Bogon_192.0.2.0/24" "Bogon_192.168.0.0/16" "Bogon_198.18.0.0/15" "Bogon_198.51.100.0/24" "Bogon_203.0.113.0/24" "Bogon_224.0.0.0/4" "Bogon_240.0.0.0/4" "Bogon_255.255.255.255/32"
6      next
7  end
```

Hier werden Adress-Gruppen für die Bogons erstellt. Anschließend werden sie der Policy zugewiesen.

```bash
1   config firewall local-in-policy
2       edit 1
3           set intf "VLAN 10 HA"
4           set srcaddr "Bogon_Addresses"
5           set dstaddr "all"
6           set service "PING"
```

```
7           set schedule "always"
8       next
9       edit 2
10          set intf "VLAN 20 HA"
11          set srcaddr "Bogon_Addresses"
12          set dstaddr "all"
13          set service "PING"
14          set schedule "always"
15      next
16  end
```

Falls nun eine private Adresse im AS auftaucht und diese Adresse versucht die FortiGate zu erreichen wird diese geblockt.