Session timeout settings auf einer Fortigate

Getestet auf 7.4.4

Dieser Artikel beschreibt, wie man die TTL-Werte von Sitzungen anpasst, wenn Portbereiche und benutzerdefinierte Dienste gleichzeitig konfiguriert sind.

- Die Sitzungs-TTL kann global mit der Variable 'default' des Befehls 'config system session-ttl' eingestellt werden. Der in der Variable „default“ festgelegte Standard-Session-Timeout kann zwischen 300 und 604.800 Sekunden liegen. Standardmäßig beträgt sie 3.600 Sekunden.
- Es ist möglich, diesen Standard-TTL-Wert für bestimmte Ports oder Portbereiche zu überschreiben, indem die 'timeout'-Variable des Befehls 'config port' verwendet wird. Die 'timeout'-Variable kann auf einen Wert zwischen 1 und 604.800 Sekunden gesetzt werden. Standardmäßig ist sie auf 300 Sekunden eingestellt.
- Es ist auch möglich, einen benutzerdefinierten Dienst zu definieren, um entweder einen neuen Dienst zu spezifizieren oder einen bestehenden Dienst zu verfeinern. In diesem Fall ersetzt der Wert, der in der Variable „session-ttl“ des Befehls „config firewall service custom“ festgelegt wird, den unter 2) definierten TTL-Wert der Sitzung.
- Der Befehl 'config firewall service custom' erlaubt auch die Änderung des UDP-Session-Timeouts über die Variable 'udp-idle-timer'. Der Wert, der in dieser Variable gesetzt wird, ersetzt den globalen Wert, der in der Variable 'udp-idle-timer' des Befehls 'config system global' gesetzt wird und standardmäßig 180 Sekunden beträgt.
- Der Sitzungs-TTL-Wert kann auch im Rahmen der Firewall-Richtlinie geändert werden. Dies gilt für jeden Verkehr, der über die Firewall-Richtlinie abgewickelt wird. Nachfolgend eine Illustration:

```
config firewall policy
                edit <policy_id>
                        set session-ttl <>
                next
           end
```

Im folgenden Beispiel wird für den Verkehr über TCP-Port 1194 eine Sitzungs-TTL von 310 Sekunden und für den Verkehr über UDP-Port 1194 eine Sitzungs-TTL von 60 Sekunden verwendet.

Wenn VDOMs aktiviert sind, muss der Befehl pro VDOM ausgeführt werden (ohne Global).

```
config system session-ttl
set default 300
config port
    edit 1194
        set protocol 6
        set timeout 50
        set start-port 1194
        set end-port 1194
    next
  end
end
```

Oder SSH. Wobei hier die Sessions 3h aktiv bleiben.

```
    edit 2
            set protocol 6
            set timeout 10800
            set start-port 22
            set end-port 22
        next
```

Die Übersetzung der Protokollnummern findet man hier.