Knowledge Base

Session Timeouts auf den Fortigate Firewalls (FortiOS v4.x)

Datum	24/05/2011 10:55:00
Hersteller	Fortinet
Modell Type(n)	Alle Fortigates
Firmware	v4.x
Copyright	Boll Engineering AG, Wettingen
Autor	sy
Dokument-Version	1

Situation:

Auf der Fortigate werden Sessions, über die für eine bestimmte Zeit kein Traffic läuft, aus Sicherheitsgründen gelöscht. Hiervon werden aber weder Client noch Server benachrichtigt. Dieses kann zu unerwarteten Verbindungsabbrüchen führen. Als Beispiel hierfür sei eine Terminalserver-Verbindung genannt, bei der der Benutzer „kurz“ einen Kaffee trinken geht und danach weiterarbeiten möchte. Bei der ersten Eingabe seitens des Nutzers fällt die Bildschirmanzeige wieder zurück auf das Login-Fenster und der Nutzer muss sich neu anmelden. Dieses passiert, weil die Fortigate die Session aus ihrer Session Table gelöscht hat und nun keine weiteren Pakete dieser Session zulässt. Der Benutzer kann erst wieder weiterarbeiten, wenn eine komplett neue Session aufgebaut wird (stateful inspection firewall).

Der default Wert für die time-to-live (TTL) liegt bei der Fortigate mit v4.0 bei 3600 Sekunden, also einer Stunde. Wurde die Konfiguration jedoch bereits von der Version v2.5 upgedatet, so wird die Konfiguration noch den alten default Wert von 300 Sekunden (5 Minuten) beinhalten.

Folgender Artikel beschreibt die verschiedenen Möglichkeiten die Session Time-to-live (TTL) Werte auf der Fortigate zu verändern.

Achtung:
Eine Erhöhung der Timeout-Werte kann die Performance der Fortigate negativ beeinflussen. Deshalb sollte bei einer stark ausgelasteten Fortigate der TTL-Wert nur dort geändert werden, wo es wirklich notwendig ist.

Lösung:

Ab der FortiOS Version 4.0 gibt es insgesamt vier verschiedene Möglichkeiten den Session-TTL Wert zu setzen:

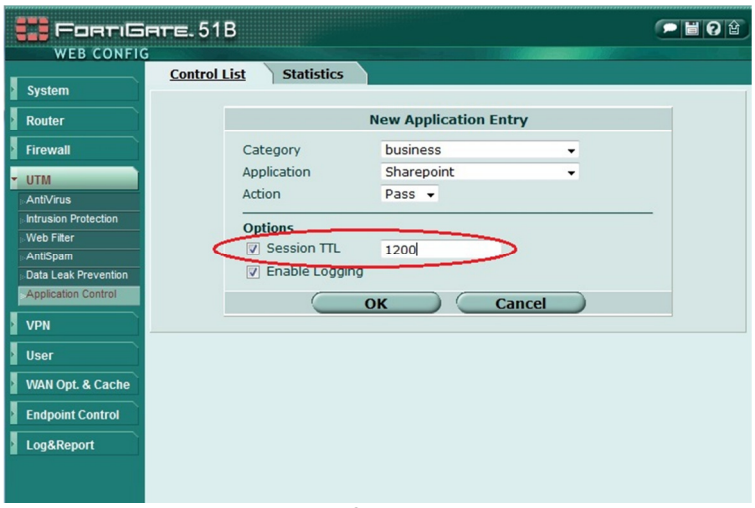
- über das Application Control (neu)
- über die Firewall Policy (neu)
- über die TTL-Einstellungen pro Port (nur übers CLI)
- über die Veränderung des allgemeinen default Werts (nur übers CLI)

Der TTL kann in allen Konfigurationen einen Wert zwischen 300 und 604800 Sekunden (5 Minuten und 7 Tagen) annehmen.

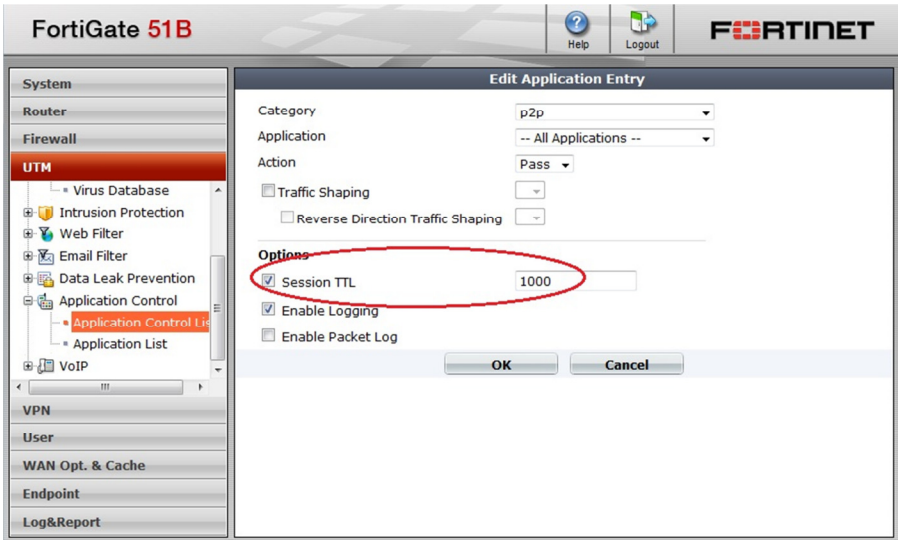
Session Timeouts auf den Fortigate Firewalls (FortiOS v4.x)

Konfiguration der Session TTL im Application Control

Ueber das Application Control können spezifischen Applikationen eine eigene TTL zugeordnet werden. Wichtig ist natürlich, dass die Applikation mit der entsprechend gesetzten TTL in einer Application Control Liste enthalten ist, welche wiederum in der Firewall Policy aktiviert ist, über die diese Applikation auch wirklich läuft. Nur dann zeigt diese Einstellung Wirkung auf die gewünschte Applikation. Die TTL kann im WebGUI gesetzt werden:

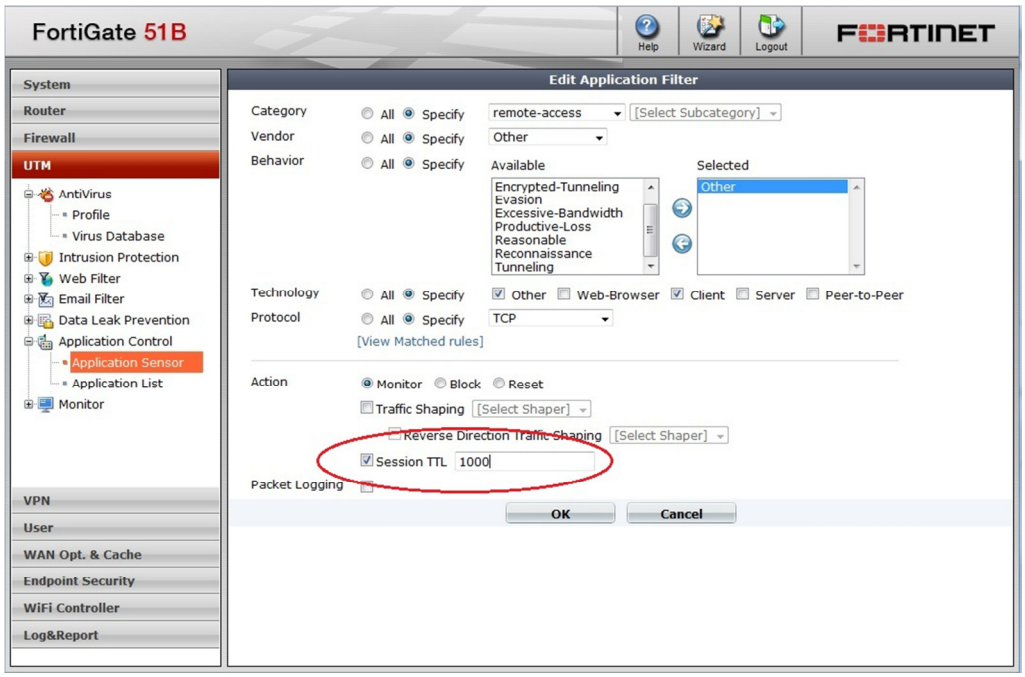


v4.0 / v4.1



v4.2

Session Timeouts auf den Fortigate Firewalls (FortiOS v4.x)



v4.3

Konfiguration der Session TTL in der Firewall Policy

Wird das Application Control nicht genutzt, kann der TTL Wert auch über die Firewall Policy gesetzt werden. Dieser TTL Wert wirkt sich dann auf alle Sessions aus, die über diese Firewall Policy laufen.

Die Konfiguration des TTL Wertes in der Firewall Policy erfolgt über das CLI:

```
config firewall policy
  edit <idx>             # wobei <idx> die ID der Firewall Policy ist.
  set session-ttl 1000   # Der Wert wird in Sekunden angegeben. „0“ bedeutet,
end                      # dass der Wert nicht gesetzt ist, also keinen Einfluss
                         # nimmt. Das ist auch die Default Einstellung.
```

Konfiguration der Session TTL in den „system“-Einstllungen

Eine weitere Möglichkeit, die Default TTL zu verändern, ist das Setzen der TTL pro Port. Dieses geschieht wiederum im CLI.

Mit der Version 4.0 kann hierüber aber lediglich der TTL-Wert für TCP-Sessions angepasst werden.

Version 4.0:

```
config system session-ttl
  config port
    edit <port>          # Angabe des TCP-Ports für den der TTL gesetzt wird
      set timeout 1000   # Angabe der TTL in Sekunden
  end
end
```

Session Timeouts auf den Fortigate Firewalls (FortiOS v4.x)

Ab der Version v4.1 können sowohl die TTL-Werte von TCP-Sessions als auch von UDP-Sessions angepasst werden. Ebenfalls kann der TTL-Wert nicht nur pro Port sondern auch gleich für eine ganze Portrange geändert werden. Die Syntax der CLI-Befehle hat sich dementsprechend komplett geändert.

Version 4.1-4.3

```
config system session-ttl
  config port
    edit <idx>          # Index für diesen Eintrag (ist einfach eine Nummer)
      set protocol <prot>     # Nummer des IP-Protokolls (TCP=6, UDP=17)
                          # Wichtig ist, dass das Protokoll vor den Ports
                          # konfiguriert wird
      set start-port xx # Erster Port aus dem Portrange
      set end-port  yy  # Letzter Port aus dem Portrange
                          # Soll nur ein einzelner Port angepasst werden ist
                          # Startport = Endport
      set timeout  1000 # Angabe der TTL in Sekunden
  end
end
```

Konfiguration des Default Session TTL für alle Verbindungen

Letztlich kann eine Default Session TTL konfiguriert werden, die immer dann verwendet wird, wenn nichts anderes vorgesehen ist. Dieser Defaultwert wirkt sich bei v4.0 nur auf TCP, ab v4.1 auch auf UDP und SCTP Sessions aus.

```
config system session-ttl
  set default 600       # Angabe der TTL in Sekunden
end
```

Mehrdeutige / sich überschneidende Konfigurationen

Was passiert, wenn sich die Konfigurationen nun aber überschneiden? Zum Beispiel also eine Applikation über die Fortigate läuft, die im Application Control eine eigene TTL konfiguriert hat, zugleich aber auch in der entsprechenden Firewall Policy eine andere TTL konfiguriert wird und auf dem Port, den die Applikation nutzt, eine dritte TTL konfiguriert wurde.

In so einem Fall nimmt die Fortigate NICHT automatisch die kürzeste oder längste TTL, sondern die TTL der spezifischsten Konfiguration. Und dabei ist das Application Control spezifischer als die Firewall Policy, die Firewall Policy spezifischer als die Port Konfiguration und die wiederum spezifischer als der Default Wert:

1. TTL im Application Control
2. TTL in der Firewall Policy
3. TTL in der Port Konfiguration
4. Default TTL