

Traffic Shaping

Network üzerinde çeşitli durumlarda belirli bir trafik tipine, servis tipine, ip bloğuna veya benzeri bir kaynak gruba belirli bir bant genişliği tahsis edilmesi gerekebiliyor. Bu işlem için ilgili cihaz üzerinde trafiği şekillendirmek, dolayısıyla Traffic Shaping tanımları yapmak gerekecektir. Bu yazıda Fortigate FW üzerinde Traffic Shaping konfigürasyonunun nasıl yapıldığı açıklanmaya çalışılacaktır.

Traffic Shaping ile herhangi iki LAN arayüzü arasındaki trafik şekillendirilebileceği gibi LAN – WAN (Internet) arasındaki trafik de şekillendirilmek istenebiliyor. Bu yazıda şekillendirme işleminin iki farklı şekilde nasıl gerçekleştirilebileceği açıklanmaya çalışılacaktır. FW üzerinde tanımlı VLAN10 ve VLAN20 arayüzlerinin internete çıkış trafiği üzerinde uygulama yapılacaktır. Bu süreçte ilgili VLAN arayüzlerinin internet erişimi için **Default Static Route** ve **Firewall Policy** tanımlarının yapıldığı varsayılarak açıklamalar yapılacaktır (Bu tanımları ve daha fazlasını **Lab** dizini altında bulabilirsiniz).

Traffic Shaping konfigürasyonu için ilk olarak “**Policy&Objects → Traffic Shaping**” yolu takip edilmelidir. Açılan sayfada kullanıcıyı **Traffic Shaper**, **Traffic Shaping Policies** ve **Traffic Shaping Profiles** olmak üzere üç farklı sekme karşılayacaktır. Bu sekmelerin anlamlarına bakıldığında;

- **Traffic Shapers**, belirli bir trafik grubuna tahsis edilmesi için trafik önceliği ve garanti edilen minimum ve maksimum bant genişliği gibi çeşitli niteliklerin belirlendiği alandır.
- **Traffic Shaping Policies**, herhangi bir arayüz üzerindeki belirli bir kaynağın (belirli ip adresleri, servisler vs. olabilir) trafiğini şekillendirmek için Policy tanımlarının yapıldığı alandır.
- **Traffic Shaping Profiles**, çıkış arayüzündeki bant genişliğinin ne kadarlık kısmının tahsis edileceği ve hangi kaynaklara ne oranda tahsis edileceğini **yüzdelik dilimlerle** kategorize etmek için kullanılan alandır.

Traffic Shapers

Traffic Shaping Policies

Traffic Shaping Profiles

+ Create New

Edit

Clone

Delete

Search

Q

Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization
Shared 5			
guarantee-100kbps	100.00 kbps	1.05 Gbps	0 bps
high-priority		1.05 Gbps	0 bps
low-priority		1.05 Gbps	0 bps
medium-priority		1.05 Gbps	0 bps
shared-1M-pipe		1.02 Mbps	0 bps

1- Bant Genişliği Kbit Olarak Tahsis Edilerek

- Traffic Shaping konfigürasyonu için ilk olarak kullanılacak maximum bant genişliği için **Traffic Shaper** tanımları yapılması gerekiyor. Traffic Shaper tanımları için “**Policy&Objects → Traffic Shaping → Traffic Shapers → Create New**” yolu takip edilmelidir. Burada;
 - o **Type**: tanımlanacak Traffic Shaper tanımının kullanım tipini belirlemek için kullanılıyor.
 - **Shared**, bir grup kullanıcının/ip grubunun trafiği şekillendirilmek istendiğinde kullanılan Traffic Shaper tanımıdır.
 - **Per IP Shaper**, **Shared** olarak tanımlanan Traffic Shaper tanımında **her bir her bir kullanıcının trafiği şekillendirilmek istendiğinde** kullanılıyor. Örnek olarak bir Shared tanımında bir gruba atanan bant genişliğinin tamamını tek bir kullanıcı kullanmaya çalışabilir. Bir gruba tahsis edilen bant genişliği üzerinde kullanıcı bazlı kısıtları belirtilmek için kullanılıyor.
- **Shared Traffic Shaper** tanımları yapılmak istendiğinde;

- **Name:** Traffic Shaper için bir isim tanımı yapılmalıdır.
- **Traffic Priority:** Her ne kadar Traffic Shaper ile belirli bir ip grubuna bant genişliği tahsis ediliyor olsa da aynı ip grubuna birden fazla Traffic Shaping tanımı uygulanmış olabilir. Bu durumda hangi Traffic Shaping trafiğine öncelik verileceğinin belirlenmesi için öncelik tanımı yapılması gerekiyor.
- **Bandwidth Unit:** Tahsis edilecek bant genişliğinin hangi birimde belirtileceğini tanımlamak için kullanılıyor.
- **Maximum Bandwidth:** bir ip grubuna tahsis edilecek bant genişliğinin en yüksek ne kadar olabileceğinin belirtildiği alandır.
- **Guaranteed Bandwidth:** bir ip grubuna tahsis edilecek bant genişliğinin en düşük ne kadar olabileceğinin belirtildiği alandır.
- **DSCP:** IP başlığında TOS alanında belirtilen alandır. Paketleri L3 üzerinde sınıflandırmak, öncelik kazandırmak için kullanılmaktadır. Traffic Shaping Policies kısmında trafiğin gönderileceği (Outgoing Interface) arayüz üzerinde öncelik kazandırılarak iletilmesini sağlamak için kullanılmaktadır. Detaylar için “**Networking-Works/CCNP-ENCORE/CCNP-09-QoS/ QoS (Quality of Service).pdf**” notlarını inceleyebilirsiniz.

Edit Traffic Shaper

Type
Shared
Per IP Shaper

Name
NewShaper

Quality of Service

Traffic priority
High

Bandwidth unit
Mbps

Maximum bandwidth
5
Mbps

Guaranteed bandwidth
2
Mbps

DSCP
011110

OK
Cancel

```

Fortinet # config firewall shaper traffic-shaper
Fortinet (traffic-shaper) # edit NewShaper
Fortinet (NewShaper) # set bandwidth-unit mb
Fortinet (NewShaper) # set maximum-bandwidth 5
Fortinet (NewShaper) # set guaranteed-bandwidth 2
Fortinet (NewShaper) # set priority high
Fortinet (NewShaper) # set diffserv enable
Fortinet (NewShaper) # set diffservcode 011110
Fortinet (NewShaper) # end

```

```

guaranteed-bandwidth  Amount of bandwidth guaranteed for this shaper (0 - 16776000). Units depend on the bandwidth-unit setting.
maximum-bandwidth     Upper bandwidth limit enforced by this shaper (0 - 16776000). 0 means no limit. Units depend on the bandwidth-unit setting.
bandwidth-unit        Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).
priority              Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.
per-policy            Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.
diffserv              Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.
overhead              Per-packet size overhead used in rate computations.

```

- **Per IP Shaper** tanımı yapılmak istendiğinde;
 - **Name:** Traffic Shaper için bir isim tanımı yapılmalıdır.

- **Bandwidth Unit:** Tahsis edilecek bant genişliğinin hangi birimde belirtileceğini tanımlamak için kullanılıyor.
- **Maximum Bandwidth:** tek bir ip/kullanıcı için tahsis edilecek bant genişliğinin en yüksek ne kadar olabileceğinin belirtildiği alandır.
- **Max concurrent connections:** tek bir kullanıcının genel olarak (TCP ve UDP) eş zamanlı oluşturabileceği maksimum oturum sayısını sınırlandırmak için kullanılmaktadır.
- **Max concurrent TCP connections:** tek bir kullanıcının eş zamanlı oluşturabileceği maksimum TCP oturumunun sayısını sınırlandırmak için kullanılmaktadır.
- **Max concurrent UDP connections:** tek bir kullanıcının eş zamanlı oluşturabileceği maksimum UDP oturumunun sayısını sınırlandırmak için kullanılmaktadır.
- **Forward DSCP:** DSCP alanı IP başlığında TOS alanında belirtilen alandır. Traffic Shaping Policies kısmında trafiğin gönderileceği (Outgoing Interface) arayüz üzerinde öncelik kazandırılarak iletilmesini sağlamak için kullanılmaktadır.
- **Reverse DSCP:** DSCP alanı IP başlığında TOS alanında belirtilen alandır. Traffic Shaping Policies kısmında gelen trafik üzerinde öncelik kazandırılarak iletilmesini sağlamak için kullanılmaktadır.

New Traffic Shaper

Type: ☐ Shared ☒ Per IP Shaper

Name:

Quality of Service

Bandwidth unit	<input type="text" value="kbps"/>
Maximum bandwidth	<input checked="" type="checkbox"/> <input type="text" value="250"/> kbps
Max concurrent connections	<input checked="" type="checkbox"/> <input type="text" value="12"/>
Max concurrent TCP connections	<input checked="" type="checkbox"/> <input type="text" value="6"/>
Max concurrent UDP connections	<input checked="" type="checkbox"/> <input type="text" value="6"/>
Forward DSCP	<input checked="" type="checkbox"/> <input type="text" value="011110"/>
Reverse DSCP	<input checked="" type="checkbox"/> <input type="text" value="011110"/>

```
Fortinet # config firewall shaper per-ip-shaper
Fortinet (per-ip-shaper) # edit NewPerIPShaper
Fortinet (NewPerIPShaper) # set bandwidth-unit kbps
Fortinet (NewPerIPShaper) # set max-bandwidth 250
Fortinet (NewPerIPShaper) # set max-concurrent-session 12
Fortinet (NewPerIPShaper) # set max-concurrent-tcp-session 6
Fortinet (NewPerIPShaper) # set max-concurrent-udp-session 6
Fortinet (NewPerIPShaper) # set diffserv-forward enable
Fortinet (NewPerIPShaper) # set diffservcode-forward 011110
Fortinet (NewPerIPShaper) # set diffserv-reverse enable
Fortinet (NewPerIPShaper) # set diffservcode-rev 011110
Fortinet (NewPerIPShaper) # end
```

max-bandwidth	Upper bandwidth limit enforced by this shaper (0 - 16776000). 0 means no limit. Units depend on the bandwidth-unit setting.
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper (0 - 2097000). 0 means no limit.
max-concurrent-tcp-session	Maximum number of concurrent TCP sessions allowed by this shaper (0 - 2097000). 0 means no limit.
max-concurrent-udp-session	Maximum number of concurrent UDP sessions allowed by this shaper (0 - 2097000). 0 means no limit.
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.

Traffic Shapers						
Traffic Shaping Policies						
Traffic Shaping Profiles						
+ Create New	Edit	Clone	Delete	<input type="text" value="Search"/>		
Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref.
Per-IP 1						
NewPerIPShaper		250.00 kbps				0
Shared 6						
NewShaper	2.00 Mbps	5.00 Mbps	0 bps		High	0
guarantee-100kbps	100.00 kbps	1.05 Gbps	0 bps		High	0

Bu süreçte VLAN'ların ilgili networklere erişimi için gerekli Static Route ve Policy tanımının yapılmış olması gerekiyor. Bu uygulamada VLAN10 ve VLAN20'ni internet erişimleri üzerinde uygulama yapılacaktır. Bu nedenle Policy ve Static Route tanımlarının aşağıdaki gibi olacaktır.

+ Create New	Edit	Clone	Delete	<input type="text" value="Search"/>		
Destination	Gateway IP	Interface	Status	Comments		
0.0.0.0/0	192.168.1.37	port1	Enabled			

+ Create New	Edit	Delete	Policy Lookup	<input type="text" value="Search"/>			Export	Interface Pair View	By Sequence
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
VLAN10_to_Internet	VLAN10	port1	VLAN10_Addr	all	always	ALL	ACCEPT	Enabled	SSL no-inspection
VLAN20_to_Internet	VLAN20	port1	VLAN20_Addr	all	always	ALL	ACCEPT	Enabled	SSL no-inspection
Implicit Deny	any	any	all	all	always	ALL	DENY		Disabled

Traffic Shaper tanımları yapıldıktan sonra artık bu tanımları bir ip grubuyla eşleştirmek için **Traffic Shaping Policy** tanımı yapılmalıdır. Burada belirli ip'lerin belirli ip'lere giden trafiklerinde, belirli servislerin trafiklerinde veya buna benzer pek çok özelleştirme işlemi yapılabilmektedir. Bunun için **"Policy&Objects -> Traffic Shaping -> Traffic Shaping Policies -> Create New"** yolu takip edilmelidir. Buradaki alanların kullanımlarına bakıldığında;

- **Traffic Shaping Policy** tanımı yapılmak istendiğinde;
 - o **Name:** Traffic Shaping Policy için bir isim tanımı yapılmalıdır.
 - o **Status:** Traffic Shaping Policy tanımının durumunu belirlemek için kullanılıyor.
 - o **Source:** uygulanacak Traffic Shaper tanımını kullanacak kaynak ip adresleri belirtilmelidir.
 - o **Destination:** uygulanacak Traffic Shaper tanımını kapsayan kaynak ip adreslerinden gönderilecek hedef ip adresleri belirtilir.
 - o **Schedule:** Bu Traffic Shaper Policy tanımının hangi zaman aralıklarında uygulanacağını belirlemek için kullanılıyor. Devreye alınmadığı takdirde varsayılanda Policy sürekli uygulanacaktır.
 - o **Service:** uygulanacak Traffic Shaper tanımının hangi servisler için geçerli olacağını belirlemede kullanılıyor.
 - o **Application:** uygulanacak Traffic Shaper tanımının hangi uygulamalar veya uygulama kategorileri (Application Control) için geçerli olacağını belirlemede kullanılıyor.

Select Entries

Application
 Category
 Group

[+ Create](#)

- o **URL Category:** bu kısımda ise uygulanacak Traffic Shaper tanımının hangi kategorideki web sayfalarında geçerli olacağını belirlemede kullanılıyor.

- **Outgoing Interface:** Filtrenin uygulanacağı çıkış arayüzün tanımlandığı alandır. Traffic Shaper Policy bu arayüzden çıkarılan trafıklere uygulanacaktır.
- **Apply Shaper:** trafiği şekillendirmek için kullanılacak Shaper tanımlarının belirtildiği alandır. Burada çıkış arayüzü olarak belirtilen arayüzden trafikler çıkarılırken belirtilen Share Traffic Shaper tanımı uygulanabildiği gibi bu arayüze gelen trafıklere de aynı veya farklı bir Shared Traffic Shaper tanımı yapılabiliyor. Ek olarak burada tanımlanan Traffic Shaper Policy tanımı içerisindeki kullanıcıların kişisel bağlamda kısıtlamak için oluşturulan Per-IP Shaper tanımı da belirtilebiliyor.
- **Assign Shaping Class ID:**

New Traffic Shaping Policy

Name
VLAN10_to_Internet_Shaper
Status
Enabled Disabled
Comments
Write a comment... 0/255

If Traffic Matches:

Source
VLAN10_Addr
Destination
all
Schedule
Service
ALL
Application
FaceTime SIP
URL Category
Business Games Internet Telephony Online Meeting

Then:

Outgoing interface
port1
Apply shaper
Shared shaper
NewShaper
Reverse shaper
NewShaper
Per-IP shaper
NewPerIPShaper
Assign shaping class ID

OK
Cancel

```

Fortinet # config firewall shaping-policy
Fortinet (shaping-policy) # edit 1
new entry '1' added
Fortinet (1) # set name VLAN10_to_Internet_Shaper
Fortinet (1) # set srcaddr VLAN10_Addr
Fortinet (1) # set dstaddr all
Fortinet (1) # set service ALL
Fortinet (1) # set application 24426 34640
Fortinet (1) # set url-category 20 49 76 95
Fortinet (1) # set dstintf port1
Fortinet (1) # set traffic-shaper NewShaper
Fortinet (1) # set traffic-shaper-reverse NewShaper
Fortinet (1) # set per-ip-shaper NewPerIPShaper
Fortinet (1) # end

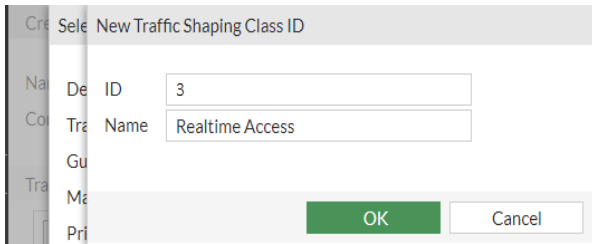
```

Bu tanımların ardından ayarlandığı üzere bant genişliği tahsis edildiği kaynaklara adanacaktır. Unutulmamalıdır ki burada ayarlanan bant genişliği kullanılmadığı takdirde diğer dahi diğer kullanıcılara paylaştırılmadan bekletilecektir. Bu nedenle Traffic Shaping tanımı yapılırken dikkatli olunmalıdır.

2- Bant Genişliği Yüzdelik Olarak Tahsis Edilerek (Traffic Shaping Profile)

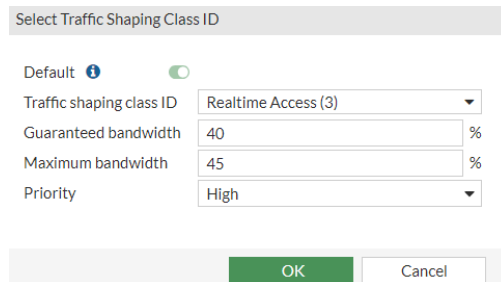
Traffic Shaping Profile konfigürasyonu çıkış arayüzünde şekillendirilmek istenen trafiğin toplam bant genişliğine göre % kaç oranda tahsis edileceğini belirlemek ve bu trafiği kategorize etmek için kullanılmaktadır. Yani Shaper tanımıyla kıyaslandığında Traffic Shaping Profile tanımı için trafiği **bant genişliği bazında değil de yüzdelik olarak** ayarlamak istendiğinde kullanılan tanım olarak açıklayabiliriz. Traffic Shaping Profile konfigürasyonuna bakıldığında;

- 3- İlk olarak **“Policy&Objects -> Traffic Shaping Profiles -> Create New ->”** yolu takip edilerek burada bir Profile tanımına isim verilmelidir.
- 4- Profile tanımına isim verildikten sonra **“Policy&Objects -> Traffic Shaping Profiles -> Create New -> Traffic Shaping Classes -> Create New -> Traffic shaping class ID -> Create”** yolu takip edilerek bant genişliği ayrılacak her bir trafik grubu için **Class ID** tanımlarının oluşturulması gerekiyor. Ben uygulamamda Realtime trafiğe öncelik vermek istediğim için iki tane Class ID tanımı yapıyorum. İkinci Class ID tanımı Defaut yani Realtime trafiğin dışındaki trafikler için kullanılacaktır.



```
Fortinet # config firewall traffic-class
Fortinet (traffic-class) # edit 3
Fortinet (3) # set class-name "Realtime Access"
Fortinet (3) # next
Fortinet (traffic-class) # edit 4
Fortinet (4) # set class-name "Default Access"
Fortinet (4) # end
```

- 5- Class ID tanımları oluşturulduktan sonra artık trafiklere Class bazında ayrılacak bant genişlikleri ve öncelik tanımları yapılabilir. Bunun için **“Policy&Objects -> Traffic Shaping Profiles -> Create New -> Traffic Shaping Classes -> Create New”** yolu takip edilerek burada hangi Class ID’ye ne kadar (toplam bant genişliğinin %’si olarak) bant genişliği tahsis edileceği belirlenmelidir.
 - a. Komut satırında Default (şekillendirilecek trafik dışında kalan trafikler **“set default-class-id <Class ID>”**) trafikler için kullanılacak Class ID tanımının belirtilmesi zorunludur.



```
Fortinet # config firewall shaping-profile
Fortinet (shaping-profile) # edit "MyNetworkX"
new entry 'MyNetworkX' added
Fortinet (MyNetworkX) # set default-class-id 4
Fortinet (MyNetworkX) # config shaping-entries
Fortinet (shaping-entries) # edit 1
new entry '1' added
Fortinet (1) # set class-id 3
Fortinet (1) # set guaranteed-bandwidth-percentage 40
Fortinet (1) # set maximum-bandwidth-percentage 45
Fortinet (1) # set priority high
Fortinet (1) # next
```

```
Fortinet (shaping-entries) # edit 2
new entry '2' added
Fortinet (2) # set class-id 4
Fortinet (2) # set priority medium
Fortinet (2) # set guaranteed-bandwidth-percentage 60
Fortinet (2) # set maximum-bandwidth-percentage 80
Fortinet (2) # set priority medium
Fortinet (2) # end
Fortinet (MyNetworkX) # end
```

Edit Traffic Shaping Profile

Name MyNetworkX
Comments

Traffic Shaping Classes

+ Create New
Edit
Delete
Set as Default
Search

Default	Class ID	Guaranteed Bandwidth	Maximum Bandwidth	Priority
Yes	Default Access (4)	60%	80%	Medium
	Realtime Access (3)	40%	45%	High

- 6- Traffic Shaping Profile tanımı yapıldıktan sonra artık Profile tanımının ilgili arayüze bağlaması gerekiyor. Bunun için “**Network → Interfaces → <Interface ID>**” yolu takip edilerek ilgili arayüz altında “**Traffic Shaping → Outbound Shaping Profile**” kısmında tanımlanan Profile tanımı uygulanmalıdır. Burada “**Outbound Bnadwidth**” kısmıyla arayüzün toplam bant genişliği yerine sadece belirli bir kısmı da Traffic Shaping Profile tanımına tahsis edilebiliyor.

Traffic Shaping

Outbound shaping profile ☒ MyNetworkX

Outbound bandwidth ☒ 10000 kbps

```
Fortinet # config system interface
Fortinet (interface) # edit port1
Fortinet (port1) # set egress-shaping-profile "MyNetworkX"
Fortinet (port1) # set outbandwidth 10000
Fortinet (port1) # next
Fortinet (interface) # end
```

- 7- Traffic Shaping Profile tanımı, ilgili çıkış arayüzüne (WAN – Port1) uygulandıktan sonra son adımda öncelik verilecek kaynakların belirtileceği Traffic Shaping Policy tanımının hazırlanması gerekiyor. Burada kolaylık sağlaması adına VLAN10 için hazırladığımız tanımdan farklı olarak “**Apply Shaper**” kısmı yerine “**Assign Shaping Class ID**” kısmında, oluşturduğumuz Shaper Class ID tanımı belirtiyoruz.

Edit Traffic Shaping Policy

Name
VLAN20_to_Internet_Shaper
Status
Enabled Disabled
Comments
Write a comment... 0/255

If Traffic Matches:

Source
VLAN20_Addr
+
x

Destination
all
+
x

Schedule
Schedule
Service
ALL
+
x

Application
FaceTime
SIP
+
x
x

URL Category
Business
Games
Internet Telephony
Online Meeting
+
x
x
x
x

Then:

Outgoing interface
port1
+
x

Apply shaper
Assign shaper class ID
Traffic shaping class ID
Realtime Access (3)

OK
Cancel

```

Fortinet # config firewall shaping-policy

Fortinet (shaping-policy) # edit 2
new entry '2' added

Fortinet (2) # set name VLAN20_to_Internet_Shaper

Fortinet (2) # set srcaddr VLAN20_Addr

Fortinet (2) # set dstaddr all

Fortinet (2) # set service ALL

Fortinet (2) # set application 24426 34640

Fortinet (2) # set url-category 20 49 76 95

Fortinet (2) # set dstintf port1

Fortinet (2) # set class-id 3

Fortinet (2) # end

```


Kaynaklar

- <https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/933502/shared-traffic-shaper>
- <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/107907/limiting-bandwidth-with-traffic-shaping>
- <https://www.youtube.com/watch?v=64Y5zG9oQ7U>
- <https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/626246/traffic-shaping-profiles>
- <https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/297431/traffic-shaping>
- <https://community.fortinet.com/t5/Support-Forum/Traffic-shaper-vs-Shaping-profile/td-p/206591>
- <https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/626246/traffic-shaping-profiles>