

## FaaS : Firewall as a Service

Protect, control and monitor everything that transits to and from your network!



**Protect, control and monitor everything that transits to and from your network with our full managed Firewall as a Service (FaaS)!**

The firewall is a central component of corporate security, because it secures the flow of information on the IT network. With our “FaaS” solution, each company, with its specific needs and security criteria, benefits from a appropriate response to protect itself from external attacks, which are themselves constantly evolving.

Firewalls need to be regularly updated to guarantee optimum protection against new intrusion methods, but they also need to be managed on a daily basis to analyze alerts.

Our complete service takes care of these primordial aspects, and many others!

### Our special extras:

- ◆ Least opening : “only open what is needed in order to control and limit the information that could leave the company”
- ◆ Protection of users’ Internet browsing via the firewall to block anything that could be dangerous for the company (phishing, viruses, etc.)
- ◆ Continuity of service: the firewalls in our service are changed every 5 years on average, so that we can guarantee that our products are in line with market standards.
- ◆ Enhanced protection: alerts raised on all our customers result in the deployment of security patches for all of them!

## The benefits of FaaS :

- ◆ Firewall adapted to your needs (several models available / upgradable or downgradable) with constant updates and support
- ◆ Fortinet Unified Threat Protection Bundle (App Control, Intrusion Prevention System, Web Filtering, Antivirus with Advanced Malware Protection, and DNS Filter) included
- ◆ Additional management layer with automatic firewall updates
- ◆ Hardware warranty with same-day replacement (during working hours)
- ◆ Automatic back-up management
- ◆ Log management and retention
- ◆ H24 firewall logging and alert management to our support services
- ◆ Replacement of hardware every 5 years with a new-generation model
- ◆ Multiple options available: analysis and remediation in the event of an incident, secure remote connection via SSLVPN or IPsec, OTP solution, on-demand activity and compliance reports, redundancy and balancing on several Internet lines via SD-WAN, etc.

## How do you choose between purchasing and FaaS?

	Purchase			Our FaaS solution	
	Without licence	Basic licence	UTP licence	FaaS Light	FaaS
Firmware update	X	✓	✓	✓ Automatic and regular	✓ Automatic and regular
Hardware warranty	X	✓ (sans SLA)	✓ (sans SLA)	✓ Next Business Day (standard model)	✓ Next Business Day (standard model)
Advanced Protection Pack (Webfiltering, IPS, AV, SSL Inspection, DNS Filter...)	X	X	✓	X	✓
Automated backup, versioning and centralised management	X	X	X	✓	✓
Logs	7 days (Forticloud)	7 days (Forticloud)	7 days (Forticloud)	45 days	45 days
Reports	✓ (Forticloud basic)	✓ (Forticloud basic)	✓ (Forticloud basic)	✓ Customizable	✓ Customizable
Lifecycle management	X	X	X	✓ Up/downgrade, new model exchange	✓ Up/downgrade, new model exchange

## Which firewall to choose?

	FaaS 40 Light*	FaaS 40	FaaS 60	FaaS 100	FaaS > 100 (Specific case)*
Number of users <sup>1</sup>	< 15	< 25	20-70	50 - 300	*
Number of VLANs <sup>1</sup>	< 5	< 5	< 30	4096	4096
VPN Site to Site <sup>1</sup>	< 5	< 5	< 20	< 200	*
Internal bandwidth <sup>1</sup>	< 500 Mbps	< 500 Mbps	< 1 Gbps	< 10 gbps	*
SD-Wan (internet redundancy or line aggregation)	Not recommended	Not recommended	✓	✓	✓
Redundant power supply	X	X	X	✓	✓
Rackable	With fortirack	With fortirack	With fortirack	✓	✓
10 Gbps capable	X	X	X	✓	✓

<sup>1</sup> 4 criteria must be valid, otherwise choice of superior model or technical validation

\* technical validation required