



## Рекомендации, направленные на снижение риска полной блокировки FortiGate

**Продукт:** FortiGate с постоянными лицензиями на основной функционал

**Пример дополнительного функционала:** UTP Bundle (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare) и отдельные подписки

**Риск:** Отзыв лицензий из личного кабинета компании на сайте <https://support.fortinet.com>. Имеются подтвержденные прецеденты отзыва всех лицензий, зарегистрированных в личных кабинетах, у компаний из списка SDN (<https://sanctionssearch.ofac.treas.gov/>)

**Исключения:** В случае с сертифицированными FortiGate никаких действий предпринимать не требуется, так как у сертифицированных версий изначально отсутствует функционал удаленных коммуникаций и обновление осуществляется исключительно вручную с помощью обновлений, предоставляемых ЗАО «НИЦ»

### Последствия реализации риска:

1. Продолжает работать как раньше: FW, VPN, SD-WAN, SSL, статический WEB
2. Обнуляется поддержка и перестают обновляться базы сигнатур: APP, IPS, AV, WEB, TECH\_SUPP
3. Перестает работать динамический веб-фильтр: WEB (динамический по категориям)

### Действия до реализации риска:

В первую очередь необходимо сохранить [Entitlement](#) файлы из личного кабинета компании на сайте <https://support.fortinet.com>.

Далее необходимо развернуть [FortiManager в изолированной среде](#), загрузить в него Entitlement файлы и разрешить [обновления FortiGate](#) только с ним.

В такой конфигурации обновление баз FortiManager производится исключительно вручную и сохраняется полный функционал FortiGate даже в случае отзыва лицензий из личного кабинета до истечения срока действия подписок.

## Действия при реализации риска:

1. Если применены действия до реализации риска, то может осуществляться ручное обновление баз FortiManager и сохраняется полный функционал FortiGate, отсутствие TECH\_SUPP.
2. Если действия до реализации риска не были применены и риск реализовался, то вернуть отозванную функциональность без наличия Entitlement файлов невозможно. В таком случае имеется возможность запретить коммуникации FortiGate с серверами компании FortiNet:

```
config system autoupdate push-update
  set status disable
end
config system autoupdate schedule
  set status disable
end
config system autoupdate tunneling
  set status disable
  end
config system global
  set endpoint-control-fds-access disable
  set fds-statistics disable
  unset fgd-alert-subscription
  set security-rating-result-submission disable
end
config system fortiguard
  set service-account-id "
  set auto-join-forticloud disable
  set sandbox-region "
  set antispam-force-off enable
  set outbreak-prevention-force-off enable
end
```

## КОНТАКТЫ

ООО «УЦСБ»  
+7 (343) 379-98-34

soc@ussc.ru  
soc.ussc.ru

