



ТИПОВЫЕ ПРОБЛЕМЫ И ОШИБКИ ПРИ **ИНТЕГРАЦИИ FORTIGATE**

Никулин Алексей
SE at Fortiservice

ТИПОВЫЕ ОШИБКИ: РАЗРАБОТКА АРХИТЕКТУРЫ

1 **FortiGate не маршрутизатор,**
а устройство обеспечения
безопасности

2 Функционал должен
использоваться по мере
необходимости

3 При разработке архитектуры
внедрения не обойтись без
L2/L3 схем

4 При сложных проектах
всегда необходимо
проводить тестирование

ТИПОВЫЕ ОШИБКИ: **ПОДБОР УСТРОЙСТВА**

1 Не стоит выбирать
устройства по даташитам

3 Необходимо
проводить тесты

2 Обмен информацией о различных
показателях устройств с другими клиентами
Fortinet эффективен крайне редко

ТИПОВЫЕ ОШИБКИ: **ВЫБОР ВЕРСИИ ОС**

1

Не стоит выбирать самые новые версии. **Самое новое - не всегда самое лучшее**

2

К выбору версии операционной системы стоит подойти серьезно

ТИПОВЫЕ ОШИБКИ:

ВЫБОР ВЕРСИИ ОС

3 При выборе операционной системы можно опираться на правило:

ТЕКУЩИЙ РЕЛИЗ

Если нужны новые функции

-1 РЕЛИЗ

В общем случае

-2 РЕЛИЗА

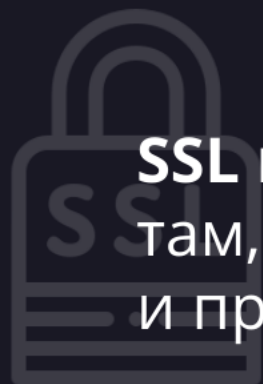
Для ЦОДов и критических инфраструктур

СОВМЕСТИМОСТЬ ВЕРСИЙ FORTIOS РАЗЛИЧНЫХ ПРОДУКТОВ FORTINET

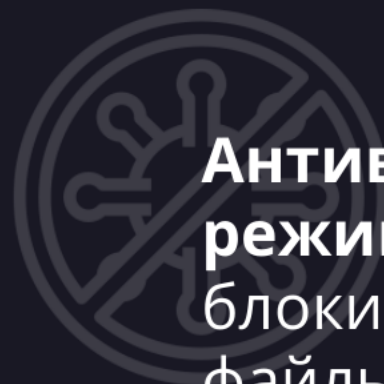
1 Для корректной работы
версии FortiOS должны быть
совместимы

2 Проверить совместимость
версий FortiOS можно с
помощью документа
Compatibility Matrix

ЧЕК ЛИСТ: НАСТРОЙКА FORTIGATE

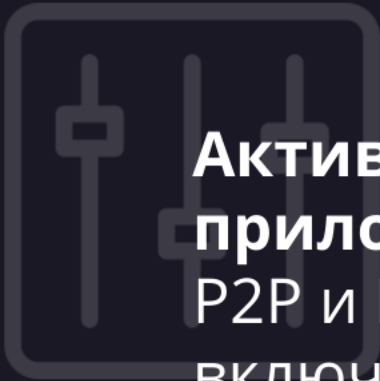


SSL инспекция включена там, где необходимо и протестирована

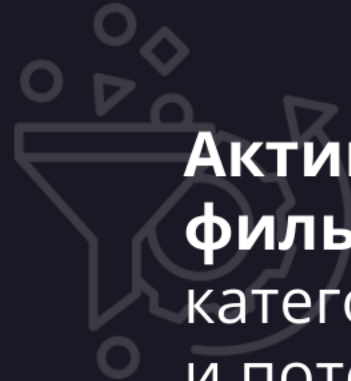


Антивирус работает в режиме Full, активирована блокировка grayware, файлы отправляются на анализ в песочницу;

ЧЕК ЛИСТ: НАСТРОЙКА FORTIGATE



Активирован контроль приложений, блокирующий P2P и Proxu приложения, включена блокировка QUIC;



Активирована веб фильтрация, блокируются категории с неприемлемым и потенциально опасным контентом;

ЧЕК ЛИСТ: НАСТРОЙКА FORTIGATE



IPS используется и донастраивается.

Сигнатуры используются в зависимости от защищаемых ресурсов (включение всех сигнатур без разбора может сильно влиять на производительность устройства)

ЧЕК ЛИСТ: НАСТРОЙКА FORTIGATE



DoS Policy используются на внешних интерфейсах, значения для различных treshhold подбираются в зависимости от привычного трафика сети

ЧЕК ЛИСТ: НАСТРОЙКА FORTIGATE



Используется привязка к AD и механизмы SSO для контроля трафика на уровне пользователей;



Используется сервис **Security Rating**, который проверяет текущие настройки, и предоставляет лучшие практики по ним;

ЧТО ДЕЛАТЬ ДАЛЬШЕ?



Периодический
аудит конфигурации



Интеграция
с другими решениями



Дальнейшее
обучение

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

ОСНОВНЫЕ ВАЖНЫЕ МОМЕНТЫ

АНГЛИЙСКИЙ ЯЗЫК

Нужно уверенное знание

СОЗДАНИЕ ЗАЯВОК

Необходимо выставить подходящий приоритет — от этого зависит SLA

ОПИСАНИЕ ПРОБЛЕМЫ

Как можно более точно и конкретно

ВАШ ОТВЕТ

Не затягивайте с ответом техподдержке

ПОПЫТАЛИСЬ РЕШИТЬ САМИ?

Прикрепите полученные данные к заявке

ТРЕБОВАНИЯ ТЕХПОДДЕРЖКИ

Будьте готовы выполнять действия из кукбуков, собирать требуемую диагностику и т. д.

УДАЛЕННЫЕ СЕССИИ

Эффективный механизм ускорения решения проблемы

FORTISERVICE

- Выполняем полный цикл работ — от выявления потребностей до поддержки внедренного решения
- Регулярно выпускаем образовательные материалы



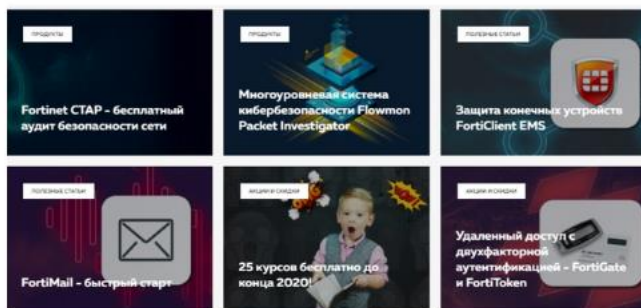
FORTISERVICE

- Выполняем полный цикл работ — от выявления потребностей до поддержки внедренного решения
- Регулярно выпускаем образовательные материалы



FORTISERVICE

- Выполняем полный цикл работ — от выявления потребностей до поддержки внедренного решения
- Регулярно выпускаем образовательные материалы



FORTISERVICE

- Выполняем полный цикл работ — от выявления потребностей до поддержки внедренного решения
- Регулярно выпускаем образовательные материалы

КОНТАКТЫ

15

sales@fortiservice.ru

www.fortiservice.com

8 (499) 288 84 90 (МСК)

8 (812) 317 79 16 (СПБ)

VK: /FORTISERVICE

FB: /FORTISERVICE

HABR: /COMPANY/FORTISERVICE

