

Контрольные вопросы по практическим работам (сценариям) Континент 4

Сценарий №5 "Настройка правил фильтрации"

1. Какие два типа контентной фильтрации реализованы в Континент 4? В чём их принципиальное различие?
2. По каким параметрам правила межсетевого экрана трафик распределяется по цепочкам обработки? Как происходит выбор цепочки?
3. Что произойдёт с трафиком, попавшим в цепочку контроля приложений (без вскрытия SSL), если приложение не будет обнаружено?
4. Перечислите основные рекомендации по порядку расположения правил фильтрации в списке (относительно узких/широких классификаторов и ресурсозатратности механизмов).
5. Как в Менеджере конфигурации создать сетевой объект типа «Сеть»? Какие поля необходимо заполнить?
6. Как создать первое разрешающее правило «Allow all»? Какие параметры указываются и на какие узлы безопасности оно устанавливается?
7. Каким образом проверяется работоспособность правила «Allow all» после его применения?
8. Опишите последовательность действий для создания правила, разрешающего DNS-запросы со всех хостов учебного стенда к DNS-серверу (10.0.1.200).
9. Опишите процесс настройки SSL-инспекции для проверки HTTPS-трафика на наличие вирусов. Какие сертификаты создаются, экспортируются и куда устанавливаются?
10. Как проверить работу созданных правил фильтрации? Какие команды и действия используются для проверки доступности хостов, работы SSL-инспекции и просмотра журнала сетевой безопасности?

Сценарий №6 "Настройка COV в составе UTM-узла безопасности"

1. Что такое БРП и какова структура правила БРП?
2. Какие значения может принимать поле «действие» в правиле БРП?
3. Как включить компонент «Система обнаружения вторжений» на узле безопасности sgw?
4. Что такое переменные COV и как изменить переменную HOME_NET?
5. Как создать профиль COV? Какие основные параметры указываются?
6. Как настроить привязку правил БРП в профиле COV? Какие способы противодействия используются?
7. Как создать политику COV и назначить её на узел безопасности?
8. Как проверить правильность настройки созданного профиля COV?
9. Какие изменения необходимо внести в правило фильтрации №6 для работы COV?
10. Как проверить работу сигнатур COV и найти информацию о сработавшей сигнатуре в БРП?