ОПИСАНИЕ МОДУЛЕЙ SKYBOX SECURITY

ТИПЫ ЛИЦЕНЗИЙ И ВАРИАНТЫ УСТАНОВКИ SKYBOX SECURITY

Март 2020

SKYBOX®
SECURITY

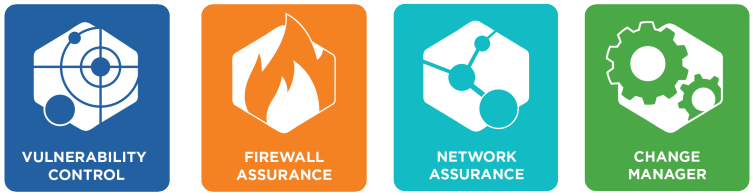
КРАТКОЕ ОПИСАНИЕ РЕШЕНИЯ

Состав функциональных модулей

Skybox Security представляет собой программную аналитическую платформу, которая имеет модульную функциональную архитектуру. Каждый модуль отвечает за реализацию определенного функционала и может приобретаться и работать самостоятельно.

В состав Skybox Security входят следующие модули:

- Network Assurance;
- Firewall Assurance;
- Change Manager;
- Vulnerability Control.



Краткое описание функциональных модулей

Network Assurance

Модуль **Network Assurance** предназначен для работы с сетевыми устройствами (L3). Данный модуль может функционировать как самостоятельно, так и в комбинации с другими модулями. Модуль лицензируется по количеству сетевых устройств, включая межсетевые экраны. Минимальная лицензия включает 10 сетевых устройств.

Основными возможностями модуля Network Assurance (NA) являются:

1. сбор конфигураций со всех поддерживаемых сетевых устройств (L3) и автоматические построение карты сети;
2. контроль соответствия конфигураций сетевых устройств заданным стандартам конфигурирования и лучшим практикам, включая локальные принятые правила конфигурирования;
3. вычисление и визуализация на карте сети возможных путей/маршрутов прохождения заданного типа трафика с демонстрацией разрешающих и запрещающих правил/настроек, которые задействованы для данного пути/маршрута;
4. создание политики сетевого доступа (сетевого сегментирования) и автоматический контроль ее исполнения как в масштабах всей модели сети, так и на уровне настроек отдельных устройств.

Firewall Assurance

Модуль Firewall Assurance предназначен для работы с межсетевыми экранами, и может функционировать как самостоятельно, так и в комбинации с другими модулями. Межсетевыми экранами для Firewall Assurance могут выступать как непосредственно межсетевые экраны, так и другие поддерживаемые сетевые устройства, использующие списки доступа (ACL). Skybox Security распознаёт наиболее полный список поставщиков межсетевых экранов и понимает сложные наборы правил даже для виртуальных и облачных межсетевых экранов, а также учитывает сигнатуры IPS. Модуль лицензируется по количеству межсетевых экранов.

Модуль отображает все межсетевые экраны в едином окне, осуществляет их постоянный мониторинг на соответствие политикам, оптимизирует правила межсетевых экранов, осуществляет непрерывный мониторинг настроек межсетевых экранов.

Основными возможностями модуля Firewall Assurance (FA) являются:

1. Автоматический сбор конфигураций межсетевых экранов и непрерывный мониторинг настроек, включая отслеживание всех изменений;
2. Оптимизация списков доступа межсетевых экранов:
    - выявление затененных, избыточных и дублирующихся правил;
    - выявление редко используемых правил и объектов;
    - формирование рекомендаций по оптимизации конфигураций.
3. Контроль соответствия конфигураций межсетевых экранов заданным стандартам конфигурирования и лучшим практикам, включая локальные правила конфигурирования, а также указание причины несоответствия вплоть до конкретных правил на конкретных устройствах:
    - Выявление правил, содержащих any в 2 или 3 полях, в поле сервис и т.д.
    - Выявление настроек, противоречащих рекомендациям производителей с точки зрения безопасности;
    - Выявление правил, разрешающих передачу паролей в открытом виде и т.д.
4. Создание политики сетевого доступа (зон безопасности) и автоматический контроль ее исполнения (встроены стандарты PCI DSS, NIST) на уровне зон безопасности межсетевых экранов с указанием причины несоответствия вплоть до конкретных правил на конкретных устройствах.

Change Manager

Change Manager (CM) является дополнением к модулю Firewall Assurance, при этом количество лицензий CM всегда соответствует FA.

CM позволяет контролировать и автоматизировать процесс изменения правил доступа от заведения заявки до ее выполнения, и гарантирует то, что все изменения произведены в полном соответствии с принятым регламентом предоставления сетевого доступа.

Основными возможностями модуля Change Manager (CM) являются:

1. создание workflow на изменение сетевого доступа за счет встроенной системы заявок или интеграции с внешними системами:
    - предоставление или изменение сетевого доступа;

- периодический пересмотр правил сетевого доступа;
- выявление изменений правил и настроек, выполненных без соответствующей заявки или согласования;

2. автоматическое выделение устройств, на которых необходимо произвести изменение;
3. формирование рекомендаций по вносимым изменениям конфигураций МЭ при изменении сетевых доступов;
4. автоматическое применение планируемых изменений правил МЭ (в частности, Check Point, Palo Alto, Fortinet, Cisco);
5. автоматическая оценка влияния планируемых изменений на политику сетевого доступа и безопасного конфигурирования, а также (в случае наличия модуля Vulnerability Control) на защищенность ИТ-активов с точки зрения появления дополнительных уязвимостей, связанных с изменением.

Vulnerability Control

Модуль Vulnerability Control является модулем работы с уязвимостями и лицензируются по числу ИТ-активов (например, серверы или рабочие станции (по сути, сканируемые IP-адреса)), в отношении которых необходимо производить анализ и расчет векторов атак. Минимальная лицензия включает пакет до 100 активов.

Vulnerability Control объединяет данные со всех сканеров, систем патч-менеджемента и систем инвентаризации, информацию о потенциальных уязвимостях и источниках угроз, коррелирует данные об уязвимостях с картой сети и позволяет визуализировать вектора возможных атак.

Основными возможностями модуля Vulnerability Control (VC) являются:

1. Автоматический сбор информации об ИТ-активах (имеющиеся уязвимости, актуальный состав и версии ПО) из сканеров, систем инвентаризации и патч-менеджмента;
2. Автоматический сбор конфигураций сетевых устройств и построение карты сети (на сетевые устройства при этом должны быть приобретены лицензии VC);
3. Расчет возможных векторов атак с учетом настроек сетевого оборудования, включая активированные сигнатуры IPS;
4. Выявление вновь появляющихся уязвимостей в период до/между сканированиями (ежедневно обновляемая собственная база);
5. Приоритезация найденных уязвимостей с учетом:
    - Возможности ее реальной эксплуатации в условиях конкретной сети и ее настроек;
    - Сведений о частоте эксплуатации данной уязвимости (на основе подписок Threat Intelligence Feeds);
    - Сведении о ценности актива, содержащего данную уязвимость и т.д.
    - Критичности уязвимости;
    - Наличие готовых инструментов атак (exploits), направленных на эксплуатацию конкретной уязвимости;
    - Факты атак, в ходе которых зафиксирована эксплуатация конкретной уязвимости.
6. Формирование рекомендаций по устранению уязвимостей с возможностью реализации workflow на базе встроенной системы заявок.