

ОПИСАНИЕ МОДУЛЕЙ SKYBOX SECURITY

ТИПЫ ЛИЦЕНЗИЙ SKYBOX SECURITY

Март 2020





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 автоматическое 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 ану 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 лицензируется 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.

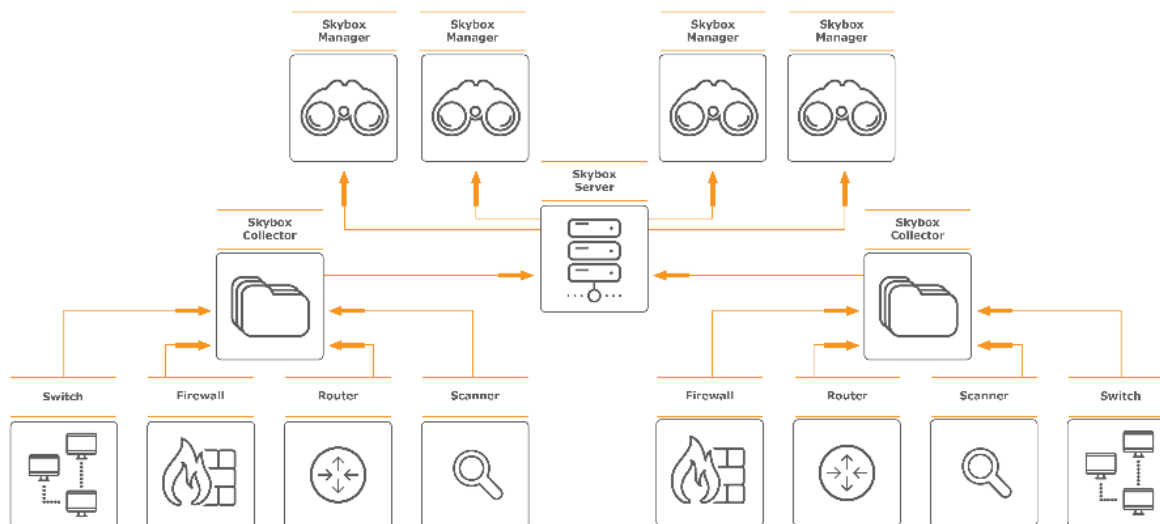
Vulnerability Control объединяет данные со всех сканеров, систем патч-менеджмента и систем инвентаризации, информацию о потенциальных уязвимостях и источниках угроз, коррелирует данные об уязвимостях с картой сети и позволяет визуализировать вектора возможных атак.

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);
 - Сведения 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.

Архитектура решения

В общем виде архитектура решения представлена на рисунке.



Сервер Skybox является базовым компонентом, и лицензия на него приобретается независимо от количества и состава приобретаемых модулей.



ДОСТУПНЫЕ ТИПЫ ЛИЦЕНЗИЙ SKYBOX SECURITY

№	Модули и компоненты	Краткое описание функционала	Наименование	SKU/Артикул		
				Лицензии	Обновление контента	Техническая поддержка
1.	Skybox Server	Базовый компонент, который приобретается независимо от количества и состава модулей.	Skybox Enterprise Server SW (unlimited Managers and Collectors)	SBV-ES		TS-S-SBV-ES
2.	Network Assurance	1. Сбор конфигураций сетевого оборудование и построение карты сети	Network Assurance 10 n-node pack	NA-10	CON-VD-NA-10	TS-S-NA-10
		2. Анализ соответствия конфигураций сетевых устройств заданным стандартам конфигурирования и лучшим практикам, включая локальные принятые правила конфигурирования	Network Assurance 100 n-node pack	NA-100	CON-VD-NA-100	TS-S-NA-100
		3. Контроль сетевого доступа (сетевого сегментирования) и автоматический контроль ее исполнения как в масштабах всей модели сети, так и на уровне настроек отдельных устройств	Network Assurance 1,000 n-node pack	NA-1K	CON-VD-NA-1K	TS-S-NA-1K
3.	Firewall Assurance	1. Оптимизация правил доступа (ACL) межсетевых экранов: <ul style="list-style-type: none"> • выявление затененных, избыточных и дублирующих правил; • выявление редко используемых правил и объектов; • формирование рекомендаций по оптимизации конфигураций. 2. Анализ правил доступа (ACL): <ul style="list-style-type: none"> • 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. 3. Контроль политики сетевого доступа (зон безопасности) на уровне зон безопасности межсетевых экранов.	Firewall Assurance 1 firewall pack	FA-1	CON-VD-FA-1	TS-S-FA-1
			Firewall Assurance 10 firewall pack	FA-10	CON-VD-FA-10	TS-S-FA-10
			Firewall Assurance 100 firewall pack	FA-100	CON-VD-FA-100	TS-S-FA-100
			Firewall Assurance 500 firewall pack	FA-500	CON-VD-FA-500	TS-S-FA-500
4.	Change Manager	1. создание workflow на изменение сетевого доступа за счет встроенной системы заявок или интеграции с внешними системами 2. автоматическое выделение устройств, на которых необходимо произвести изменение и формирование рекомендаций по вносимым изменениям правил доступа 3. автоматическое применение планируемых изменений правил МЭ (в частности, Check Point, Palo Alto, Fortinet)	Change Manager 1 firewall pack	CM-1	CON-VD-CM-1	TS-S-CM-1
			Change Manager 10 firewall pack	CM-10	CON-VD-CM-10	TS-S-CM-10
			Change Manager 100 firewall pack	CM-100	CON-VD-CM-100	TS-S-CM-100
			Change Manager 500 firewall pack	CM-500	CON-VD-CM-500	TS-S-CM-500
5.	Vulnerability Control	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 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 уязвимостей 6. Формирование рекомендаций по устранению уязвимостей с возможностью реализации workflow на базе встроенной системы заявок	Vulnerability Control 100 asset pack	VC-100	CON-VD-VC-100	TS-S-VC-100
			Vulnerability Control 1,000 asset pack	VC-1K	CON-VD-VC-1K	TS-S-VC-1K
			Vulnerability Control 10,000 asset pack	VC-10K	CON-VD-VC-10K	TS-S-VC-10K
			Vulnerability Control 50,000 asset pack	VC-50K	CON-VD-VC-50K	TS-S-VC-50K

