МЕТОДИКА ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ УСТРОЙСТВ КЛАССА NGFW 3.0

JET SECURITY TEAM

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Сетевые функции			
Режимы работы	Работа в режиме L3 (Routing Mode)	1. Выбрать режим функционирования L3 2. Настроить IP-адресацию MGMT-интерфейса и статический маршрут (при необходимости) 3. Настроить IP-адресацию Internal/External-интерфейсов, маршрут по умолчанию 4. Настроить правило доступа для разрешения трафика INT->EXT (ETH2->WAN) 5. Настроить правило Source NAT (Many-to-One) для выхода в интернет для VLAN Eth2 6. Настроить на тестовой рабочей станции в качестве шлюза по умолчанию INT-интерфейс тестируемого МСЭ 7. Проверить доступ к интернет-ресурсам (запустить команду ping 8.8.8.8, открыть ya.ru через браузер) 8. Убедиться в наличии событий доступа с тестовой рабочей станции	1. Выход в интернет работает 2. События появляются в логах
	Fail Close/Fail Open (настройка поведения устройства при высокой нагрузке)	1. Изучить документацию и функционал системы	Должна быть возможность настраивать поведение системы при выскокой нагрузке целиком или для отдельных модулей. В режиме Fail Close система должна закрывать доступ при срабатывании условий, а в режиме Fail Open — оставлять доступ открытым
Маршрутизация	Возможность указывать исходящий интерфейс при настройке маршрутизации	1. Создать маршрут с явно указанным исходящим интерфейсом 2. Отправить трафик, который должен использовать этот маршрут	Пакеты должны следовать указанным маршрутом и использовать указанный исходящий интерфейс
	Приоритизация маршрутов (Administrative Distance)	1. Настроить 2 протокола маршрутизации (например, OSPF, iBGP) 2. Изменить приоритет, чтобы iBGP был приоритетнее OSPF 2. Передать трафик, который должен использовать эти маршруты.	Система должна выбирать маршруты с более низким значением AD для передачи трафика.
	Поддержка FullView (маршрутизация)	1. Изучить документацию и функционал системы	МСЭ должен поддерживать Fullview
	ECMP	1. Изучить документацию и функционал системы	Система должна поддерживать распределение трафика между маршрутами в ECMP с различными весами
	BFD	1. Настроить BFD для мониторинга состояния маршрутов	BFD должен корректно обнаруживать и реагировать на изменения

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
			состояния маршрутов
	Протоколы маршрутизации	1. Проверить поддержку различных протоколов маршрутизации (OSPF, BGP, RIP и др.)	Система должна успешно работать с выбранными протоколами маршрутизации
	Ограничения для поддерживаемых динамических протоколов	1. Проверить, есть ли ограничения для используемых динамических протоколов	Должны быть ясны ограничения для каждого протокола
Интерфейсы	VXLAN	1. Изучить документацию и функционал системы	Технология VXLAN должна поддерживаться системой
	LACP	1. Настроить LACP для соединения с другим устройством 2. Передать трафик через LACP-канал	LACP-канал должен корректно обрабатывать трафик
Внешние каналы	Резервирование канала (ISP Redundancy)	1. Настроить два WAN-канала к разным провайдерам с резервированием 2. Отключить активный канал и проверить переключение на резервный	Трафик должен переключаться на резервный канал без потерь данных
	Сколько ISP поддерживается	1. Изучить документацию и функционал системы	Зафиксировать количество поддерживаемых ISP
	Статическая балансировка трафика при использовании ISP Redundancy	1. Настроить два WAN-канала к разным провайдерам с резервированием 2. Настроить статическую балансировку для WAN-линков с использованием весов 3. Передать трафик через устройство и проверить распределение по линкам	Трафик должен быть равномерно распределен между линками в соответствии с настройками статической балансировки
	Потери пакетов при выходе из строя одного линка при использовании балансировки трафика (LoadSharing Active/Active) при использовании ISP Redundancy	1. Настроить два WAN-канала к разным провайдерам с резервированием 2. Настроить статическую балансировку для WAN-линков с использованием весов 3. Отключить 1 из линков и проверить потери пакетов	Потери пакетов должны быть минимальными при выходе из строя одного линка. Зафиксировать потери
	Механизмы мониторинга физических линков при использовании ISP Redundancy	1. Изучить документацию и функционал системы	Зафиксировать поддерживаемые механизмы мониторинга линков
Базовые функции	Поддержка виртуальных контекстов	1. Настроить виртуальные контексты и передать трафик через них	Устройство должно корректно обрабатывать трафик в виртуальных контекстах
	VRF	1. Создать и настроить VRF 2. Назначить интерфейсы указанным VRF	Пакеты должны правильно маршрутизироваться внутри соответствующих VRF

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Базовые функции	Настройка Proxy ARP	1. Включить Proxy ARP для определенного интерфейса 2. Отправить трафик на сеть, для которой включен Proxy ARP	Аппаратура должна успешно отвечать на ARP-запросы относительно адресов в Proxy ARP
	Поведение устройства при обновлении правил/применении политики	1. Произвести обновление правил или применение новой политики 2. Проверить передачу трафика в процессе обновления правил/применения политики	Устройство должно корректно применять новые правила или политики, минимизируя перерыв в обслуживании
	Netflow	1. Изучить документацию и функционал системы	Устройство должно поддерживать отправку данных по протоколу Netflow
	Функционал Anti-spoofing	1. Настроить защиту Anti-Spoofing	Устройство должно выполнять защиту от Spoofing-атак
	NTP	1. Включить NTP на устройстве 2. Настроить параметры NTP	Устройство должно синхронизировать время
	Мониторинг состояния блоков питания	1. Изучить документацию и функционал системы	Зафиксировать поддерживаемые механизмы мониторинга состояния блоков питания
	Поддержка Graceful Restart для протоколов динамической маршрутизации	1. Изучить документацию и функционал системы	Устройство должно поддерживать отправку сообщений Graceful Restart для протоколов динамической маршрутизации
	Выгрузка/загрузка конфигураций в виде текстовых файлов	1. Выполнить выгрузку конфигураций в текстовом виде 2. Выполнить загрузку конфигураций в текстовом виде	Устройство должно выгружать и загружать конфигурации в виде текстовых файлов
	SNMP	1. Изучить документацию и функционал системы	Устройство должно поддерживать функцию SNMP
	Страна происхождения производителя	1. Изучить документацию и опросить вендора.	Указать страну происхождения производителя
	Наличие ТОРП-платформ	1. Изучить документацию и опросить вендора.	Вендор должен иметь ТОРП-платформы, доступные для заказа
	Сертификат ФСТЭК	1. Изучить документацию и опросить вендора.	Должен быть сертификат ФСТЭК
	Сертификат ФСБ	1. Изучить документацию и опросить вендора.	Должен быть сертификат ФСБ
	Наличие дополнительного функционала: DLP, WAF, SandBox и др.	1. Изучить документацию и функционал системы.	Перечислить наличие дополнительного функционала (модулей), не упомянутого в тестах
	QoS	1. Изучить документацию и функционал системы	Система должна поддерживать QoS

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
QoS	Применение QoS политик отдельно для интерфейсов	1. Настроить QoS-политики для отдельных интерфейсов 2. Передать трафик через интерфейсы и проверить применение QoS	QoS-политики должны корректно применяться к трафику на отдельных интерфейсах
	Применение QoS политик для зон (zones)	1. Настроить QoS-политики для зон 2. Передать трафик через зоны и проверить применение QoS	QoS-политики должны корректно применяться к трафику в зонах
Функции МСЭ			
МСЭ (L4)	Использование зон безопасности в политиках ACL	**Проверка правил Allow** 1. Настроить правило доступа к интернет-ресурсам, указав: Source Zone Destination Zone Source Destination Service (например, HTTPS) 2. Выполнить обращение к заданным ресурсам 3. Убедиться, что заданные ресурсы доступны 4. Убедиться в наличии событий доступа с тестовой рабочей станции **Проверка правил Deny** 1. Настроить правило доступа, блокирующее доступ к интернет-ресурсам, указав: Source Zone Destination Zone Source Destination Service (например, HTTPS) 2. Выполнить обращение к заданным ресурсам 3. Убедиться, что заданные ресурсы недоступны 4. Убедиться в наличии событий блокировки с тестовой рабочей станции	**Проверка правил Allow** 1. Доступ до заданного ресурса работает 2. События появляются в логах **Проверка правил Deny** 1. Доступ до заданного ресурса не работает 2. События появляются в логах
	Использование интерфейсов в политиках ACL	**Проверка правил Allow** 1. Настроить правило доступа к интернет-ресурсам, указав: Source Interface Destination Interface Source Destination Service (например, HTTPS) 2. Выполнить обращение к заданным ресурсам 3. Убедиться, что заданные ресурсы доступны 4. Убедиться в наличии событий доступа с тестовой рабочей станции	**Проверка правил Allow** 1. Доступ до заданного ресурса работает 2. События появляются в логах **Проверка правил Deny** 1. Доступ до заданного ресурса не работает 2. События появляются в логах

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
МСЭ (L4)		**Проверка правил Deny** 1. Настроить правило доступа, блокирующее доступ к интернет-ресурсам, указав: Source Interface Destination Interface Source Destination Service (например, HTTPS) 2. Выполнить обращение к заданным ресурсам 3. Убедиться, что заданные ресурсы недоступны 4. Убедиться в наличии событий блокировки с тестовой рабочей станции	
	Возможность включения интерфейсов в зоны	1. Создать новую зону и включить в нее интерфейсы 2. Создать новую политику ACL, используя созданную зону в качестве параметра	Зона с интерфейсами должна быть доступна для выбора в политике ACL
	Drag&Drop при работе с объектами и политиками	1. Попытаться переместить объект (например, IP-адрес) или политику, используя Drag&Drop	Объект или политика должны успешно перемещаться при использовании Drag&Drop
	Stateful Inspection	1. Активировать Stateful Inspection 2. Провести тестовую передачу корректного трафика через NGFW 3. Провести передачу «некорректной» сессии.	NGFW должен отслеживать состояние соединения и принимать решения на основе этой информации. Корректный трафик пропускается, некорректный блокируется
	Ускорение обработки трафика	1. Узнать, какие механизмы ускорения трафика используются	Предоставлена информация об используемых механизмах
	NAT-правила для определенных правил МСЭ	1. Создать NAT-правило для конкретной политики МСЭ 2. Протестировать соответствующий трафик	NAT должен корректно применяться к трафику, соответствующему указанной политике МСЭ
МСЭ (L4)	Расписание действия правил МСЭ	1. Создать правило ACL с установкой расписания 2. Проверить, что правило применяется только в указанные временные интервалы	Правило должно применяться только в установленные временные рамки
	Поддержка временных правил МСЭ	1. Создать правило ACL с установкой времени существования 2. Проверить, что правило применяется в заданное время существования и автоматически удаляется после его завершения	Правило должно применяться только в установленное время существования и после окончания данного времени автоматически удаляться или отключаться

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
МСЭ (L4)	Просмотр Implicit-правил	1. Перейти в раздел настроек Implicit-правил 2. Проверить список Implicit-правил	Implicit-правила должны быть видны и доступны для просмотра
	Управление Implicit-правилами	1. Попробовать изменить настройки или отключить Implicit-правило	Если это разрешено, то настройки Implicit-правила должны быть изменены или оно должно быть отключено
	Hit Count для каждого правила	1. Перейти в раздел статистики или логов 2. Проверить, что каждое правило имеет счетчик (Hit Count)	Каждое правило должно иметь Hit Count, отображающий количество срабатываний
	Поиск правил по объекту	1. Использовать сущность «Объект» при поиске правил 2. Проверить результаты поиска	Поиск с использованием сущности «Объект» должен возвращать соответствующие правила
	Проверка правил на дубликаты	1. Попробовать создать дубликат правила 2. Проверить систему на предмет предупреждения или блокировки дубликата	Система должна предотвращать создание дубликатов правил или предоставлять предупреждение
	Объекты для создания правил	Типы объектов: IP host IP range Пользовательские группы Сервисы и порты Протоколы Типы приложений Типы устройств (например, маршрутизаторы, серверы) Географические области (если применимо)	В результатах указать поддерживаемые типы объектов
	Блокировка по GeoIP	Тест-кейс для блокировки по стране 1. Включить GeoIP-блокировку 2. Выбрать конкретную страну для блокировки 3. Передать трафик с устройства, находящегося в выбранной стране Тест-кейс для исключения определенных IP из блокировки 1. Включить GeoIP-блокировку 2. Создать исключение для конкретных IP-адресов 3. Передать трафик с устройства, находящегося в выбранной стране, но входящего в исключенные IP	Тест-кейс для блокировки по стране Доступ должен быть заблокирован в соответствии с настройками GeoIP Тест-кейс для исключения определенных IP из блокировки Доступ должен быть разрешен для исключенных IP, несмотря на блокировку GeoIP
	Наличие поля «Комментарий» на каждом правиле	1. Изучить документацию и функционал системы	Устройство должно поддерживать поля «Комментарий» на каждом правиле
NAT	Очередность выполнения NAT	1. Изучить документацию и функционал системы	Выяснить, в какой очередности выполняются правила NAT для всех поддерживаемых типов (например, 1. SNAT, 2. DNAT и т.д.)

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Возможность выбора интерфейса, на котором будет осуществляться NAT	1. Создать правило NAT и выбрать конкретный интерфейс для его применения 2. Передать трафик, соответствующий правилу NAT	NAT должен быть применен только на выбранном интерфейсе
	Source NAT	1. Создать Source NAT-правило 2. Передать трафик, требующий применения Source NAT	Исходный адрес в заголовке пакета должен быть заменен на указанный в Source NAT-правиле
	Destination NAT	1. Создать Destination NAT-правило 2. Передать трафик, требующий применения Destination NAT	Целевой адрес в заголовке пакета должен быть заменен на указанный в Destination NAT-правиле
PBR (Policy Based Routing)	PBR	1. Проверить наличие и функциональность PBR	Должна быть поддержка и корректная работа PBR
	ISP Redundancy с провайдером при использовании PBR	1. Настроить PBR для отказоустойчивого линка с провайдером 2. Имитировать отказ одного из линков	Трафик должен успешно переключиться на рабочий линк, обеспечивая отказоустойчивость
Функции NGFW/UTM			
IPS	IPS	Тест-кейс проверки детектирования 1. Уточнить перечень актуальных/часто используемых уязвимостей 2. Выбрать 2-3 уязвимости для эксплуатации 3. На защищаемом сервере развернуть уязвимые версии ПО для последующей эксплуатации (при необходимости) 4. Настроить правило доступа к защищаемому серверу 5. Настроить правило DNAT для публикации сервисов защищаемого сервера 6. Настроить механизм SSL Inspection для защищаемого сервера (импортировать сертификат сервера и т. д.) 7. Настроить проверку трафика к защищаемому серверу средствами модуля IPS (при обнаружении атаки должно выполняться только журналирование) 8. С внешней рабочей станции произвести эксплуатацию уязвимости из п.2 на защищаемом сервере (например, с помощью Metasploit) Тест-кейс проверки блокировки 1. Настроить проверку трафика к защищаемому серверу средствами модуля IPS (при обнаружении атаки должна выполняться блокировка) 2. С внешней рабочей станции произвести эксплуатацию уязвимости из п.2 тест-кейса проверки детектирования на защищаемом сервере (например, с помощью Metasploit)	Тест-кейс проверки детектирования 1. Эксплуатация уязвимостей выполнена успешно 2. В журналах IPS зарегистрированы события обнаружения сетевых атак Тест-кейс проверки блокировки 1. Эксплуатация уязвимостей неуспешна 2. В журналах IPS зарегистрированы события блокировки сетевых атак
	Возможность выбора определенной группы сигнатур для защиты	1. Выбрать группу сигнатур, например, только для ОС Linux 2. Передать трафик, содержащий сигнатуры для разных ОС	Система должна применить выбранные сигнатуры и обнаружить только те, которые соответствуют ОС Linux
	Создание исключений	1. Создать правило блокировки 2. Добавить исключение для конкретного IP, сигнатуры или других параметров 3. Передать трафик, соответствующий правилу с исключением	Трафик, соответствующий исключению, должен быть разрешен

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Создание самописных сигнатур	1. Перейти в раздел создания сигнатур 2. Создать новую самописную сигнатуру 3. Применить сигнатуру к трафику, содержащему соответствующий паттерн	Система должна успешно применять самописную сигнатуру к трафику и обнаруживать соответствующие паттерны
	Наличие документации, описывающей синтаксис, используемый при написании сигнатуры	1. Проверить наличие документации с описанием синтаксиса для написания сигнатур	Документация должна содержать описание синтаксиса, достаточное для самостоятельного написания сигнатур
Защита от DoS	Защита от DoS	1. Проверить наличие и функциональность DOS-защиты 2. Перечислить методы защиты от DoS	Должна быть поддержка и корректная работа средств защиты от DoS-атак
	Защита от SYN-flood	1. Настроить защиту SYN-flood 2. Проверить срабатывание защиты SYN-flood	Устройство должно выполнять защиту от SYN-flood-атак
	Защита от HTTP-flood	1. Настроить защиту HTTP-flood 2. Проверить срабатывание защиты HTTP-flood	Устройство должно выполнять защиту от HTTP-flood-атак
	Защита от ICMP-flood	1. Настроить защиту ICMP-flood 2. Проверить срабатывание защиты ICMP-flood	Устройство должно выполнять защиту от ICMP-flood-атак
Application Control	Поддержка сложных правил. Например: 1. Разрешить трафик на YouTube, но запретить оставлять комментарии 2. Разрешить трафик VK, но запретить пользоваться Multimedia	1. Создать правило для разрешения трафика на YouTube и запрета оставлять комментарии 2. Создать правило для разрешения трафика в VK и запрета использования Multimedia	Трафик должен соответствовать указанным условиям
	Добавление собственных приложений	1. Добавить собственное приложение в политику 2. Протестировать трафик через это приложение	Приложение должно быть успешно добавлено и работать в соответствии с настройками политики
	Конфигурация сервисов на определенных портах	1. Настроить политику для определенных сервисов на определенных портах 2. Провести тестирование трафика	Трафик для указанных сервисов и портов должен соответствовать настройкам политики
	Политика реализации Application Control	1. Создать политику с использованием Blacklist 2. Создать политику с использованием Whitelist	Blacklist должен блокировать все, что в списке. Whitelist должен разрешать только то, что в списке
	Политика для трафика — «Неизвестный или не мог быть опознан устройством»	1. Создать политику для трафика, не опознанного устройством	Политика должна быть успешно применена к трафику, не идентифицированному устройством
	Страница оповещения для пользователя (блокировка)	1. Настроить политику с выбором портала оповещения о блокировке 2. Попробовать выход на запрещенный сайт	Пользователь должен получить уведомление о блокировке через выбранный портал
	Страница оповещения для пользователя (предупредить и продолжить)	1. Настроить политику с выбором портала оповещения «Предупредить и продолжить»	Администратор должен получить заполненную форму, пользователь должен продолжить работу после предупреждения

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		2. Попробовать выход на запрещенный сайт 3. Заполнить форму	
	Блокировка QUIC-протокола	1. Проверить, есть ли возмоэность настроить политику блокировки протокола QUIC	Должна быть возможность заблокировать трафик, использующий протокол QUIC
Antivirus	Использование сторонних сигнатур Threat Feed	1. Узнать, есть ли возможность подключить сторонний Threat Feed к антивирусному модулю	Должна быть возможность использовать сторонние сигнатуры для обнаружения вирусов
	Условия работы антивируса	1. Изучить документацию и функционал системы	Зафиксировать условия, при которых работает антивирус
	Проверка скачиваемых файлов	1. Загрузить файл с вирусом	Антивирус должен блокировать скачивание файла с вирусом
	Проверка работы антивируса по FTP	1. Передать вредоносный файл по протоколам FTP	Антивирус должен успешно обнаруживать и блокировать вредоносные файлы
	Проверка SMB	1. Узнать, проверяет ли потоковый антивирус вредоносный файл по протоколу SMB	Антивирус должен успешно обнаруживать и блокировать вредоносные файлы по SMB
	Типы файлов	1. Передать различные типы файлов, включая .exe, .doc, .pdf и др.	Антивирус должен успешно обнаруживать и блокировать вредоносные файлы различных типов
	Проверка файлов в архивах без паролей	1. Передать вредоносные файлы, архивированные без паролей	Антивирус должен успешно сканировать и блокировать вредоносные файлы в архивах без паролей
	Проверка файлов в архивах с паролями	1. Передать вредоносные файлы, архивированные с паролями	Антивирус должен успешно сканировать и блокировать вредоносные файлы в архивах с паролями
	Выбор действий для определенных типов файлов	1. Настроить правила для различных действий для определенных типов файлов 2. Передать файлы и проверить реакцию антивируса	Антивирус должен действовать согласно настроенным правилам для каждого типа файла
	Антивирусный движок	1. Узнать используемый антивирусный движок	Должна быть предоставлена информация о версии и происхождении антивирусного движка
	Поддержка добавления пользовательских хешей	1. Проверить, есть ли возможность создать собственные сигнатуры для антивируса	Должна быть возможность добавлять собственные сигнатуры
SSL Inspection	Поддерживаемые модули для SSL Inspection	1. Узнать, с какими модулями работает SSL Inspection	Предоставлена информация о поддерживаемых модулях
	Поддерживаемые протоколы	1. Узнать, какие протоколы поддерживает SSL Inspection	Предоставлена информация о поддерживаемых протоколах
	Поддержка нестандартных портов для поддерживаемых протоколов	1. Узнать, есть ли привязка к порту. 2. Можно ли настроить инспекцию на нестандартных портах (например HTTPS на порту 8443)	Система должна корректно отрабатывать при использовании нестандартных портов
	Возможность использовать сертификаты стороннего УЦ	1. Попытаться использовать сертификат от стороннего УЦ для SSL Inspection	Система должна корректно обрабатывать и использовать сторонний сертификат для SSL Inspection

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Инспектирование для отдельных пользователей	1. Создать правило SSL Inspection для конкретного пользователя 2. Передать трафик, используя учетные данные этого пользователя	SSL Inspection должен быть применен только для указанного пользователя
	Инспектирование для отдельных сайтов	1. Создать правило SSL Inspection для конкретного веб-сайта 2. Передать трафик, направленный на указанный веб-сайт	SSL Inspection должен быть применен только к трафику, направленному на указанный веб-сайт
	Поддержка Wildcard-сертификатов	1. Попытаться использовать SSL Inspection с веб-сайтом, использующим Wildcard-сертификат	SSL Inspection должен корректно обрабатывать трафик, использующий Wildcard-сертификат
	Client-Side (Outbound SSL Inspection)	1. Создать правило SSL Inspection для исходящего трафика 2. Передать трафик с клиента на внешний ресурс	SSL Inspection должен быть успешно применен к исходящему трафику
	Server-Side (Inbound SSL Inspection)	1. Создать правило SSL Inspection для входящего трафика на сервер 2. Передать трафик с внешнего источника на сервер	SSL Inspection должен быть успешно применен к входящему трафику на сервер
Веб-фильтрация	Использование собственных или сторонних списков URL	1. Загрузить собственный или сторонний список URL 2. Применить фильтрацию к трафику, содержащему URL из загруженного списка	Система должна корректно обрабатывать трафик с использованием загруженных URL
	Тип используемой базы URL	1. Узнать тип используемой базы URL (облачная или локальная)	База URL должна соответствовать выбранному типу
	Создание кастомных URL-категорий	1. Создать новую кастомную URL-категорию 2. Применить фильтрацию к трафику, содержащему URL из созданной категории	Система должна успешно обрабатывать трафик с использованием созданной кастомной URL-категории
	Переопределение категории URL	1. Переопределить категорию URL 2. Передать трафик с измененным URL	Трафик должен быть обработан согласно новой категории URL
	Страница блокировки сайта в случае наличия вируса на странице (URL-категория)	1. Проверить, есть ли URL-категория, содержащая сайты с вирусами	Система должна выдавать страницу блокировки с информацией о наличии вируса
	Настройка доступа к определенным URL/доменам	1. Создать правило для блокировки или разрешения доступа к определенным URL/доменам 2. Передать трафик, соответствующий созданному правилу	Доступ должен быть заблокирован или разрешен согласно правилу
	URL Lookup (проверка принадлежности URL к определенной категории)	1. Выполнить URL Lookup для конкретного URL 2. Сравнить результат с категорией, предполагаемой для этого URL	Результат URL Lookup должен соответствовать предполагаемой категории
	Страница блокировки/ предупреждения	1. Попробовать получить доступ к заблокированному ресурсу	Должна отобразиться страница блокировки/ предупреждения с соответствующим сообщением
	Какие списки URL использует производитель	1. Узнать, какие URL-списки использует вендор	Предоставлена информация об используемых URL-списках
Proxy (explicit/transparent)	Explicit Proxy	1. Настроить явный прокси в системе 2. Перенаправить трафик через явный прокси	Проксирование должно быть успешно выполнено, трафик должен проходить через явный прокси

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Transparent Proxy	1. Настроить прозрачный прокси в системе 2. Перенаправить трафик через прозрачный прокси	Прозрачное проксирование должно быть успешно выполнено, трафик должен проходить через прозрачный прокси
	Авторизация Kerberos	1. Проверить возможность настроить авторизацию через Kerberos	Система должна поддерживать авторизацию через Kerberos
	Страница блокировки на Captive Portal	1. Настроить блокировку с использованием Proxy 2. Попытаться получить доступ к заблокированным ресурсам	Captive Portal должен успешно отображать блокировку для попыток доступа к заблокированным ресурсам через Proxy
	Captive Portal для авторизации на Proxy	1. Настроить Captive Portal для авторизации с использованием Proxy 2. Попытаться получить доступ к ресурсам, требующим авторизации	Captive Portal должен успешно отображать страницу авторизации, и после успешной авторизации доступ к ресурсам должен быть предоставлен
Content Filtering	Контентная фильтрация	1. Настроить Content Filtering с использованием различных категорий и правил 2. Перейти на веб-сайты, относящиеся к различным категориям	Доступ к веб-сайтам должен быть ограничен в соответствии с правилами Content Filtering
	Типы файлов для фильтрации	1. Проверить список поддерживаемых файлов	Система должна поддерживать различные типы файлов
	Блокировка файлов в архивах	1. Попытаться передать/скачать архив, содержащий файлы конкретного типа	Архив должен быть заблокирован, если внутри содержится запрещенный тип файла
	Блокировка архивов внутри архивов	1. Попытаться передать/скачать архив, содержащий другой архив	Вложенный архив должен быть заблокирован, если такая настройка задана
	Запрет загрузки файлов	1. Настроить фильтры для контроля загрузки файлов 2. Попытаться загрузить файлы различных типов	Файлы должны быть успешно загружены в соответствии с установленными фильтрами
	Запрет отправки файлов	1. Настроить фильтры для контроля выгрузки файлов 2. Попытаться выгрузить файлы различных типов	Файлы должны быть успешно выгружены в соответствии с установленными фильтрами
Anti Bot	Типы защищаемого трафика	1. Узнать, для какого трафика применяется защита (входящий, исходящий и т.д.)	Тест-кейс для проверки работы с трафиком пользователей Система должна корректно работать с трафиком от разных пользователей и применять необходимые меры защиты Тест-кейс для проверки работы с защитой опубликованных серверов Система должна успешно защищать опубликованные серверы и блокировать вредоносный трафик
	Частота обновлений	1. Узнать периодичность обновлений модуля по защите от ботов у производителя 2. Проверить дату последнего обновления на текущей системе	Дата последнего обновления на текущей системе должна соответствовать заявленной периодичности обновлений
	Место хранения баз	1. Узнать, где хранятся базы системы (локально или в облаке) 2. Проверить доступность и целостность баз на текущей системе	Базы должны быть доступны и целостны в соответствии с заявленным местом их хранения
	Выявление трафика RAT	1. Проверить, что система содержит сигнатуры для трафика, связанного с RAT	В Системе должны присуствовать сигнатуры для блокировки трафика от RAT
	Выявление обращений к вредоносными URL и доменам	1. Проверить, что система содержит и обновляет списки вредоносных URL и DGA (Domain Generation Algorithm) доменов	В Системе должны присуствовать актуальные списки вредоносных URL и доменов

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Выявление IRC-коммуникаций	1. Проверить, что система содержит сигнатуры для блокировки трафика IRC-коммуникаций	В Системе должны присутствовать сигнатуры для идентификации и блокировки трафика IRC-коммуникаций
Защита почтового трафика	Защита почты	1. Проверить наличие функционала защиты почты в системе	Система должна поддерживать функционал защиты почты
	Наличие функционала MTA	1. Проверить поддержку функционала MTA (Mail Transfer Agent)	Система должна поддерживать функционал MTA
VPN и SD-WAN			
Remote Access VPN	Поддерживаемые протоколы	1. Узнать, какие протоколы поддерживает SSL Inspection	Предоставлена информация о поддерживаемых протоколах
	Интеграция с LDAP	1. Проверить возможность интеграции VPN-решения с сервером LDAP 2. Передать учетные данные пользователя из LDAP и убедиться, что аутентификация проходит успешно	Система должна успешно интегрироваться с сервером LDAP, и пользователи из LDAP должны успешно аутентифицироваться
	VPN-клиент	1. Проверить наличие собственного клиентского приложения для установки VPN-соединения 2. Убедиться, что клиентское приложение корректно устанавливается на устройство	Система должна предоставлять собственное клиентское приложение, и его установка должна быть успешной
	Автоматическое назначение IP-адреса клиенту	1. Установить VPN-соединение с сервером 2. Проверить, был ли выдан IP-адрес клиенту	VPN-сервер должен успешно выдавать IP-адрес клиенту после установки соединения
	Поддержка 2FA	1. Проверить наличие опций для настройки второго фактора аутентификации 2. Настроить второй фактор и проверить, что он требуется при установке VPN-соединения	Система должна предоставлять возможность настройки второго фактора, и его использование должно быть успешным при аутентификации
	Получение маршрутов от шлюза	1. Установить VPN-соединение с сервером 2. Проверить, был ли выдан маршрут клиенту	VPN-сервер должен успешно выдавать маршрут клиенту после установки соединения
	SPLIT Tunnel	1. Проверить наличие опции настройки Split Tunnel 2. Настроить Split Tunnel и проверить, что трафик маршрутизируется в соответствии с заданными правилами	Система должна предоставлять возможность настройки Split Tunnel, и его использование должно корректно маршрутизировать трафик
	Направление всего трафика через VPN	1. Настроить VPN-соединение с указанием направления всего трафика через шлюз 2. Проверить, что весь сетевой трафик клиента действительно проходит через VPN-шлюз. 3. Проверить, что пользователь не может самостоятельно изменить данное поведение (с помощью настроек ОС или изменение настроек клиента).	Система должна предоставлять возможность настройки направления всего трафика через VPN-шлюз, и это должно быть успешно реализовано
	Подключение к VIP-адресу кластера шлюзов	1. Подключиться к VPN-серверу в среде с использованием кластера 2. Убедиться, что подключение идет через VIP-адрес кластера	В случае использования кластера подключение к VPN-серверу должно происходить через VIP-адрес, а не через адрес отдельной ноды
	ОС для клиента	1. Проверить список поддерживаемых операционных систем для клиента VPN	VPN-клиент должен успешно устанавливаться и работать на каждой из поддерживаемых операционных систем

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Remote Access VPN		2. Убедиться, что клиент успешно устанавливается на каждой из поддерживаемых операционных систем	
	Проверка трафика на шлюзе	1. Установить VPN-соединение и передать трафик через шлюз 2. Проверить возможность анализа VPN-трафика средствами антивируса, IPS и других функций безопасности на шлюзе	Шлюз должен успешно анализировать и обеспечивать безопасность VPN-трафика средствами антивируса, IPS и других функций
	Проверка трафика на клиентском устройстве	1. Установить VPN-клиент 2. Передать трафик через VPN и проверить возможность анализа трафика средствами антивируса, IPS и других функций безопасности на клиентском устройстве	Клиентское устройство, на котором установлен VPN-клиент, должно успешно анализировать и обеспечивать безопасность VPN-трафика
	Compliance Check клиента	1. Настроить Compliance Check для определенных параметров 2. Изменить параметры и проверить реакцию системы	Система должна обнаруживать нарушения Compliance и принимать меры
	Алгоритмы шифрования	1. Проверить список поддерживаемых протоколов шифрования VPN 2. Убедиться, что каждый протокол шифрования работает корректно при установке VPN-соединения	Система должна поддерживать заявленные протоколы шифрования, и каждый из них должен работать корректно при установке VPN-соединения
	Поддержка изолированного сегмента для клиентов, не прошедших compliance check.	1. Изучить документацию и функционал системы. 2. Настроить изолированный сегмент.	Система должна предоставлять доступ только в изолированный сегмент в случае частичного прохождения compliance check. Должны быть варианты настройки прохождения (уровни) compliance check
WEB-portal VPN	Кастомизация портала	1. Зайти в административный интерфейс SSL VPN 2. Перейти в раздел настройки портала 3. Попытаться изменить цвета, логотип, фон и другие элементы портала	Изменения должны успешно сохраняться, и пользовательский интерфейс портала должен отображать внесенные кастомизации
	Типы приложений для публикации	1. Перейти в раздел настройки приложений для публикации на портале 2. Проверить, какие типы приложений можно выбрать для публикации (веб-приложения, файлы, внутренние ресурсы и т. д.)	Система должна предоставлять разнообразные типы приложений для публикации, и выбранный тип должен успешно отображаться на портале
	Публикация нескольких порталов (на разных IP-адресах)	1. Попробовать создать несколько порталов с разными настройками и IP-адресами 2. Перейти по различным IP-адресам порталов	Каждый портал должен успешно создаваться с уникальными настройками и IP-адресами, и пользователь должен иметь доступ к каждому из порталов по соответствующему IP
	Распространение через портал Remote Access Client	1. Публикация Remote Access Client на портале 2. Проверка возможности пользователей скачивать и устанавливать Remote Access Client через портал	Remote Access Client должен быть успешно опубликован на портале, и пользователи должны успешно скачивать и устанавливать его
	Публикация собственных приложений на портале	1. Попробовать опубликовать собственное приложение на портале 2. Убедиться, что пользователи могут видеть и запускать опубликованное приложение	Пользователи должны видеть и успешно запускать публикуемые на портале собственные приложения
	Авторизация пользователя по сертификату	1. Настроить портал для авторизации по сертификату 2. Аутентифицироваться на портале, предоставив сертификат	Пользователь должен успешно аутентифицироваться на портале, предоставив сертификат

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Поддержка 2FA	1. Проверить наличие опций для настройки второго фактора аутентификации 2. Настроить второй фактор и проверить, что он требуется при установке VPN-соединения	Система должна предоставлять возможность настройки второго фактора, и его использование должно быть успешным при аутентификации
2FA	2FA + Remote Access VPN с клиентом	Должен поддерживаться хотя бы один из вариантов, в случае нескольких вариантов тестируется 1 кейс на выбор. Тест-кейс для проверки поддержки 2FA (Radius) + Remote Access VPN с клиентом 1. Настроить 2FA с использованием Radius для Remote Access VPN с VPN-клиентом 2. Подключиться к VPN, введя соответствующие учетные данные и код 2FA Тест-кейс для проверки поддержки 2FA (TOTP) + Remote Access VPN с клиентом 1. Настроить 2FA с использованием TOTP для Remote Access VPN с клиентом 2. Подключиться к VPN, введя соответствующие учетные данные и TOTP-код Тест-кейс для проверки поддержки 2FA (SMS) + Remote Access VPN с клиентом 1. Настроить 2FA с использованием SMS для Remote Access VPN с клиентом 2. Подключиться к VPN, введя учетные данные и код, полученный по SMS Тест-кейс для проверки поддержки 2FA (SMTP) + Remote Access VPN с клиентом 1. Настроить 2FA с использованием SMTP для Remote Access VPN с клиентом 2. Подключиться к VPN, введя учетные данные и код, полученный по электронной почте	Указать выбраный тест-кейс, остальные из документации Тест-кейс для проверки поддержки 2FA (Radius) + Remote Access VPN с клиентом Пользователь должен успешно подключиться к VPN после ввода корректных учетных данных и кода 2FA Тест-кейс для проверки поддержки 2FA (TOTP) + Remote Access VPN с клиентом Пользователь должен успешно подключиться к VPN после ввода корректных учетных данных и TOTP-кода Тест-кейс для проверки поддержки 2FA (SMS) + Remote Access VPN с клиентом Пользователь должен успешно подключиться к VPN после ввода корректных учетных данных и SMS-кода Тест-кейс для проверки поддержки 2FA (SMTP) + Remote Access VPN с клиентом Пользователь должен успешно подключиться к VPN после ввода корректных учетных данных и кода, полученного по электронной почте
	2FA + Remote Access VPN с SSL-порталом	Должен поддерживаться хотя бы один из вариантов, в случае нескольких вариантов тестируется 1 кейс на выбор. Тест-кейс для проверки поддержки 2FA (Radius) + Remote Access VPN с SSL-порталом 1. Настроить 2FA с использованием Radius для Remote Access VPN с SSL-порталом 2. Подключиться к VPN через SSL-портал, введя учетные данные и код 2FA Тест-кейс для проверки поддержки 2FA (TOTP) + Remote Access VPN с SSL-порталом 1. Настроить 2FA с использованием TOTP для Remote Access VPN с SSL-порталом	Указать выбраный тест-кейс, остальные из документации Тест-кейс для проверки поддержки 2FA (Radius) + Remote Access VPN с SSL-порталом Пользователь должен успешно подключиться к VPN через SSL-портал после ввода корректных учетных данных и кода 2FA Тест-кейс для проверки поддержки 2FA (TOTP) + Remote Access VPN с SSL-порталом Пользователь должен успешно подключиться к VPN через SSL-портал после ввода корректных учетных данных и TOTP-кода Тест-кейс для проверки поддержки 2FA (SMS) + Remote Access VPN с SSL-порталом Пользователь должен успешно подключиться к VPN через SSL портал после

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		2. Подключиться к VPN через SSL-портал, введя учетные данные и TOTP-код Тест-кейс для проверки поддержки 2FA (SMS) + Remote Access VPN с SSL-порталом 1. Настроить 2FA с использованием SMS для Remote Access VPN с SSL-порталом 2. Подключиться к VPN через SSL-портал, введя учетные данные и код, полученный по SMS Тест-кейс для проверки поддержки 2FA (SMTP) + Remote Access VPN с SSL-порталом 1. Настроить 2FA с использованием SMTP для Remote Access VPN с SSL-порталом 2. Подключиться к VPN через SSL-портал, введя учетные данные и код, полученный по электронной почте	ввода корректных учетных данных и SMS-кода Тест-кейс для проверки поддержки 2FA (SMTP) + Remote Access VPN с SSL-порталом Пользователь должен успешно подключиться к VPN через SSL-портал после ввода корректных учетных данных и кода, полученного по электронной почте
Site-to-Site VPN	Поддерживаемые протоколы	1. Узнать, какие протоколы поддерживает SSL Inspection	Предоставлена информация о поддерживаемых протоколах
	DPD / Tunnel Test	1. Включить Dead Peer Detection (DPD) или Tunnel Test 2. Провести тестирование наличия и корректности детекции неработающего пира	Система должна успешно обнаруживать и корректно обрабатывать неработающий пир с использованием DPD или Tunnel Test
	Инструменты диагностики VPN-соединений	1. Проверить наличие инструментов для отладки и анализа состояния VPN-соединений 2. Проверить возможность просмотра логов, статуса соединений и других отладочных данных	Система должна предоставлять инструменты, облегчающие отладку и мониторинг состояния VPN-соединений
	SA lifetime	Тест-кейс для проверки SA lifetime в режиме КБ 1. Проверить, что можно задать настройки SA lifetime в режиме, измеряемом в килобайтах Тест-кейс для проверки SA lifetime в режиме секунды/минуты 1. Проверить, что можно задать настройки SA lifetime в режиме, измеряемом в секундах или минутах	Система должна поддерживать Ipsec-соединение в соответствии с установленным лимитом по килобайтам Система должна поддерживать Ipsec-соединение в соответствии с установленным временем жизни
	Аутентификация	Тест-кейс для проверки аутентификации PSK 1. Настроить Site-to-Site VPN с аутентификацией по предварительно распределенному ключу (PSK) 2. Проверить успешность установки VPN-соединения Тест-кейс для проверки аутентификации по сертификату 1. Настроить Site-to-Site VPN с аутентификацией по сертификату 2. Проверить успешность установки VPN-соединения	Тест-кейс для проверки аутентификации PSK VPN-соединение должно успешно устанавливаться с использованием аутентификации PSK Тест-кейс для проверки аутентификации по сертификату VPN-соединение должно успешно устанавливаться с использованием аутентификации по сертификату
	Исключение из VPN-трафика	1. Проверить, что есть возможность настроить исключения для определенного сервиса или другого трафика из ВПН	Должна быть возможноть настраивать исключения из VPN-трафика

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Алгоритмы шифрования	1. Проверить список поддерживаемых протоколов шифрования VPN 2. Убедиться, что каждый протокол шифрования работает корректно при установке VPN-соединения	Система должна поддерживать заявленные протоколы шифрования, и каждый из них должен работать корректно при установке VPN-соединения
	NAT-T (NAT Traversal)	1. Включить и выключить поддержку NAT-T для Site-to-Site VPN 2. Проверить, что VPN-соединение успешно работает в обоих случаях	VPN-соединение должно успешно устанавливаться и работать как с включенным, так и с выключенным NAT-T
	PFS (Perfect Forward Secrecy)	1. Проверить, что есть возможность включить PFS в настройках Site-to-Site VPN	PFS должно применяться при согласовании VPN, новые ключи должны согласовываться с использованием PFS
	NAT внутри VPN	1. Создать NAT inside VPN-правило 2. Передать трафик внутри VPN, требующий применения NAT	NAT должен быть применен к трафику внутри VPN согласно указанному правилу
	VPN со сторонними вендорами	1. Настроить Site-to-Site VPN с оборудованием другого вендора 1. Проверить успешность установки и передачи трафика через VPN	Трафик должен успешно проходить через VPN
SD-WAN	SD-WAN	1. Проверить наличие функционала SD-WAN в системе	Система должна поддерживать SD-WAN, функционал должен быть активирован
	Распределение пользователей (локальных и доменных) по каналам	1. Настроить политику SD-WAN для распределения пользователей локальных и AD по разным каналам	Система должна позволять распределять трафик от пользователей (локальных и AD) по заданным каналам
	Распределение трафика приложений/сайтов по каналам	1. Настроить политику SD-WAN для распределения трафика по определенным приложениям или сайтам в отдельные каналы	Система должна позволять распределять трафик указанных приложениий или сайтов в соответствующие каналы
	Мониторинг трафика	1. Проверить инструменты мониторинга трафика (логи, отчеты, дашборд) для оценки производительности и использования каналов	Инструменты мониторинга должны предоставлять информацию о трафике, его использовании и производительности каналов
	Типы фильтров в политиках SD-WAN	1. Запросить информацию о типах фильтров в политиках SD-WAN	Предоставлена информация о типах фильтров
Отказоустойчивость и кластеризация			
Кластеризация	Требования к нодам кластера	1. Узнать требования к нодам кластера	Предоставлена информация о требованиях к нодам кластера
	Механизмы резервирования кластера	1. Узнать протокол, используемый для обеспечения высокой доступности	Предоставлена информация об используемых протоколах
	VIP-адрес и адреса физических интерфейсов должны принадлежать одной подсети	1. Узнать требования к типам адресов нод кластера	Предоставлена информация о типах интерфейсов нод кластера
	Режим получения динамических маршрутов при работе в кластере	1. Собрать и настроить кластер 2. Включить динамическую маршрутизацию по протоколам OSPF, BGP 3. Проверить для протоколов OSPF, BGP, как устанавливается соседство с сетевым оборудованием (только с активной ноды или обе ноды сразу и с какого IP — виртуального или физического)	Проверить режимы получения динамических маршрутов. Ноды кластера должны успешно обмениваться динамическими маршрутами
	Дополнительная лицензия для кластера	1. Попытаться собрать кластер без ввода лицензий 2. Проверить, возможно ли установить кластер без лицензий	Кластер собран без использования дополнительной лицензии

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Кластеризация	Добавление сетевых интерфейсов после сборки кластера	1. Собрать кластер 2. Добавить новые интерфейсы на нодах кластера 3. Проверить, что интерфейс успешно добавлен и работает в кластере	Кластер должен поддерживать добавление новых интерфейсов после сборки без необходимости пересборки
	Поведение при отключении сетевого интерфейса	1. Отключить интерфейс на текущей мастер-ноде 2. Проверить, что мастер-нода переключается на другой узел	При отключении интерфейса на текущей мастер-ноде мастер-нода должна успешно переключиться на другой узел
	GARP	1. Провести тест, включающий изменение состояния интерфейса 2. Проверить, что GARP корректно отправляется для обновления ARP-таблицы	Система должна успешно отправлять GARP для обновления ARP-таблицы при изменении состояния интерфейса
	Время переключения между нодами	1. Выключить мастер-ноду кластера 2. Измерить время на переключение	Зафиксировать время на переключение
	Синхронизация сессий	1. Установить активную TCP-сессию 2. Изменить состояние активной ноды на пассивную 3. Проверить, разрывается ли TCP-сессия и как быстро происходит восстановление	При переключении активной ноды на пассивную TCP-сессия не должна разрываться
	Кластер системы централизованного управления	1. Запросить информацию, как система обеспечивает кластер конфигурации	Предоставлена информация о кластере конфигурации
	Кластер системы централизованного логирования	1. Запросить информацию, как система обеспечивает кластер логирования	Предоставлена информация о кластере логирования
	Просмотр состояния кластера	1. Использовать инструмент просмотра состояния кластера (например, dashboard, командную строку) 2. Проверить, что информация о состоянии кластера доступна и корректна	Должен быть предоставлен инструмент для мониторинга состояния кластера, такой как дашборд, командная строка или др.
	Тип кластера	1. Запросить информацию о поддерживаемых типах кластера	Предоставлена информация о типах кластера
	VMAC	1. Проверить поддержку VMAC	Должен поддерживаться VMAC
	Количество нод кластера	1. Запросить информацию о количестве нод кластера	Предоставлена информация о количестве нод кластера
	Защита от Split brain	1. Изучить документацию и функционал системы 2. Собрать кластер 3. Добавить новые интерфейсы на нодах кластера 4. Отключить интерфейс на текущей мастер-ноде 5. Отключить интерфейс на пассивной мастер-ноде 6. Вернуть обе ноды в активное состояние	1. Устройство должно успешно переключаться при Failover 2. Активная нода должна понимать состояние проблемной ноды
Централизованное управление и отчетность			
	Выделенный сервер управления	1. Проверить документацию и конфигурацию системы	Должен быть выделенный сервер управления, если он предусмотрен системой

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Централизованное управление	Импорт правил/политик с локального МСЭ	1. Создать локальные правила на одном из устройств 2. Использовать функцию импорта на Центре управления	Правила должны быть успешно импортированы на Центр управления
	Синхронизация настроек в кластере серверов управления	1. Проверить в документации кластеризацию на Центре управления 2. Уточнить у производителя, что конфигурация или политика на одном из серверов синхронизируется со вторым. 3. При каких условиях выполняется синхронизация, можно ли управлять этими условиями административно.	Должен поддерживаться кластер управления с автоматической синхронизацией изменений. Должны быть описаны условия синхронизации
	Установка на ВМ	1. Попробовать установить Центр управления на виртуальную машину	Установка должна быть успешной, если виртуализация поддерживается системой
	Поведение МСЭ при отключении сервера управления	1. Отключить Центр управления от сети 2. Проверить функциональность МСЭ в отсутствие связи с Центром управления	МСЭ должен продолжать работать в автономном режиме или с минимальными ограничениями
	Экспорт и резервное копирование политик	1. Использовать функцию экспорта и резервного копирования для сохранения политик	Политики должны быть успешно сохранены в формате, который позволяет их восстановить при необходимости
	Централизованное обновление встроенного программного обеспечения МЭ	1. Выяснить, есть ли возможность выполнять установку обновлений через систему управления	Устройство должно производить обновление встроенного программного обеспечения МЭ через систему управления
	Наличие web-интерфейса для доступа к компонентам, включая средства управления	1. Изучить документацию и функционал системы	Устройство должно поддерживать web-интерфейс для доступа к компонентам, включая средства управления
	Передача данных между центром управления и МЭ по защищённому каналу	1. Изучить документацию и функционал системы	Центр управления и МЭ должны поддерживать передачу данных по защищённому каналу
	Выделенный сервер логирования	1. Проверить документацию и конфигурацию системы	Должен быть выделенный сервер логирования, если он предусмотрен системой
	Режим логирования	1. Настроить логирование трафика локально 2. Проверить возможность отправки логов на централизованный сервер	Логи должны успешно отправляться на централизованный сервер, если эта функция предусмотрена
	Автоматическая выгрузка логов на сторонний сервер	1. Настроить систему для автоматической выгрузки логов на сторонний сервер	Логи должны автоматически выгружаться на указанный сторонний сервер согласно настройкам
	Формат хранения логов	1. Просмотреть документацию или настройки системы	Логи должны храниться в формате, который обеспечивает удобство анализа и соответствует требованиям безопасности
	Агрегации и корреляции событий в инциденты безопасности	1. Изучить документацию и функционал системы	Система должна предоставлять функционал для регистрации и управления инцидентами
	Модули с логированием	1. Запросить информацию о модулях с логированием	Предоставлена информация о модулях с логированием

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Логирование и отчёты	Выгрузка логов	1. Проверить наличие опции выгрузки логов 2. Выполнить выгрузку логов с устройства	Система должна предоставлять возможность выгрузки логов, процесс выгрузки должен быть успешным
	Отправка логов на сторонний сервер	1. Настроить систему на отправку логов на сторонний сервер 2. Передать трафик и проверить, что логи успешно отправляются на указанный сервер	Система должна поддерживать отправку логов на сторонний сервер, отправка логов должна быть успешной
	Типы отчетов	1. Посмотреть возможные типы отчетов	Зафиксировать типы возможных отчетов (встроенные, пользовательские)
	Автоматические отчеты (по расписанию)	1. Настроить автоматическую генерацию отчетов с определенной периодичностью 2. Подождать согласно настройкам и проверить, что отчеты генерируются автоматически	Система должна поддерживать автоматическую генерацию отчетов в соответствии с заданными настройками
	Типы логирования (вся сессия, начало сессии, выбранное кол-во пакетов и т.д.)	1. Проверить настройки логирования для всей сессии, начала сессии, выбора количества пакетов и других вариантов 2. Передать трафик и убедиться, что логирование осуществляется в соответствии с заданными параметрами	Система должна поддерживать различные варианты логирования, логи должны быть соответствующим образом настроены
Логирование и отчёты	Сетевые виджеты для мониторинга трафика	1. Проверить наличие виджетов для мониторинга трафика в системе (например, bandwidth по интерфейсам, состояние VPN-туннелей) 2. Настроить виджеты для отображения конкретных данных о трафике	Система должна предоставлять виджеты для мониторинга трафика, они должны корректно отображать выбранные данные
	Системные виджеты для мониторинга состояния устройства	1. Проверить наличие виджетов для мониторинга системы (например, загрузка CPU и памяти) 2. Настроить виджеты для отображения конкретных данных о системе	Система должна предоставлять системные виджеты, они должны корректно отображать выбранные данные
	Виджеты безопасности для мониторинга трафика	1. Проверить наличие виджетов для мониторинга трафика в системе (например, Top Threats, Top Attacker) 2. Настроить виджеты для отображения конкретных данных о трафике	Система должна предоставлять виджеты безопасности, они должны корректно отображать выбранные данные
	Журналы событий в режиме реального времени	1. Зафиксировать время какого-то события (например, прохождение определенного трафика и действия администратора) 2. Проверить соотвествующие журналы и зафиксировать время, через которое события будут отображены	Устройство должно отображать соотвествующие события в режиме реального времени или с задержкой не более чем в 1 минуту.
Интеграция			
LDAP	Использование пользователей из LDAP для создания политик	1. Импортировать пользователей из LDAP 2. Создать политику для Firewall, контент-фильтра, используя импортированных пользователей	Политики должны успешно применяться к импортированным пользователям
	Права УЗ для интеграции с LDAP	1. Проверить документацию или настройки системы для указания требуемых для УЗ прав	В результатах указать «Пройден». В столбце «Заметки» указать необходимые права УЗ.
	Поддержка более одного домена	1. Проверить документацию или настройки системы для указания количества поддерживаемых доменов	В результатах указать количество поддерживаемых доменов

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Просмотр импортированных пользователей	1. Перейти на менеджмент или GW 2. Просмотреть список импортированных пользователей	Должна быть возможность просматривать импортированных пользователей на обоих уровнях
	Kerberos	1. Проверить возможность настроить Kerberos, используя LDAP	Должна быть возможность использовать kerberos при получении данных из LDAP
	Proxy-аутентификация	1. Проверить возможность настроить Proxy-аутентификацию, используя LDAP	Должна быть возможность использовать proxy-аутентификацию с использованием данных из LDAP
	Прозрачная аутентификация	1. Проверить возможность настроить прозрачную аутентификацию, используя LDAP	Должна быть возможность использовать прозрачную аутентификацию с использованием данных из LDAP
	SAML	1. Изучить документацию и функционал системы.	Аутентификация пользователей должна быть возможна с использованием SAML
Radius	Интеграция с Radius	1. Настроить интеграцию с сервером Radius 2. Передать запросы аутентификации через устройство	Устройство должно успешно использовать сервер Radius для аутентификации
	Протоколы аутентификации при интеграции с Radius	1. Изучить документацию и функционал системы	Зафиксировать поддерживаемые протоколы аутентификации при интеграции с Radius
	Использование нескольких Radius-серверов	1. Изучить документацию и функционал системы	Зафиксировать количество поддерживаемых Radius-серверов
ICAP	Интеграция по протоколу ICAP с внешними системами	1. Настроить отправку файлов на анализ по протоколу ICAP на внешнее устройство 2. Убедиться, что файлы передаются на проверку через ICAP	ICAP должен корректно проверить файл и вернуть результат
	Возможности настройки ICAP взаимодействия	1. Изучить документацию и функционал системы 2. Настроить взаимодействие с учетом respmode.	1. Должны быть возможности настройки ожидания ответа ICAP-сервера или передачи трафика, не дожидаясь ответа. 2. Должны быть настройки поведения системы при недоступности ICAP-сервера. 3. Убедиться, что МСЭ реагирует на ответ ICAP-server
Эксплуатационные возможности			
Возможности диагностики	Модули диагностики в GUI	1. Проверить раздел «Troubleshooting» в GUI для доступных модулей	Должен быть предоставлен функционал для выявления проблем
	Модули диагностики в CLI	1. Проверить доступные команды для выявления проблем в CLI	Должны быть предоставлены команды для выявления проблем
	Доступ к логам ОС	1. Перейти к логам в операционной системе	Должна быть возможность самостоятельно просматривать логи в операционной системе
	Активация дебага отдельных модулей безопасности	1. Активировать дебаг для конкретного модуля (например, Web Filter / URL Filtering)	Дебаг должен быть успешно активирован для выбранного модуля
Обновление лицензии	Обновление кластера	1. Выполнить обновление кластера в соответствии с документацией вендора	Обновление должно проходить успешно.

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Обновление кластера без простоя	1. Выполнить обновление кластера в соответствии с документацией вендора.	Обновление должно проходить без простоя
	Резервное копирование при автоматическом обновлении	1. Узнать, происходит ли автоматическое создание резервной копии перед обновлением	Резервная копия должна быть создана автоматически
	Возможность отката к предыдущей версии	1. Попытаться выполнить откат к предыдущей версии	Откат должен быть возможен
	Доступ к дистрибутивам на сайте производителя	1. Проверить доступность и возможность скачивания обновлений с официального сайта производителя	ПО должно быть доступно для скачивания с официального сайта
	Офлайн-обновления	1. Попытаться выполнить обновление без доступа к интернету	Должна быть предусмотрена возможность офлайн-обновлений, либо процесс должен предоставить необходимые инструкции для офлайн-обновления
	Обновление с web-ресурсов производителя	1. Проверить обновление с web-ресурсов производителя	Обновления должны происходить с указанного источника
	Обновление через систему централизованного управления	1. Проверить обновление через систему централизованного управления	Обновления должны происходить с указанного источника
	Офлайн-установка лицензии (без доступа в интернет)	1. Попытаться установить лицензию без подключения к интернету	Должна быть предоставлена возможность установить лицензию без подключения к интернету
Наличие API или других инструментов для миграции правил	API	1. Проверить наличие и функциональность API	Должно быть подтверждено наличие API с подробной документацией
	Для каких модулей можно загружать политики через API	1. Выяснить, какие модули доступны для управления через API 2. Перечислить инструменты миграции, используя API, указанные в документации	Указать, для каких модулей могут быть мигрированы политики с другого решения используя API
	Массовая загрузка политик	1. Выяснить, есть ли возможность массово загрузить политики на большое число МСЭ при миграции с помощью cli, API или другим способом	Конфигурация политик должна быть успешно загружена через CLI без ошибок
	Поддержка миграции с других продуктов	1. Проверить, с каких продуктов возможна миграция	Миграция должна происходить в соответствии с документацией
Резервное копирование и восстановление	Варианты резервного копирования для Системы Управления	1. Изучить документацию и функционал системы (какие варианты бэкапов есть, что попадает под бэкап)	Устройство должно поддерживать создание резервных копий, все настройки и лицензии должны сохраняться в бэкапе
	Варианты резервного копирования для NGFW	1. Изучить документацию и функционал системы (какие варианты бэкапов есть, что попадает под бэкап)	Устройство должно поддерживать создание резервных копий, все настройки и лицензии должны сохраняться в бэкапе
	Автоматические резервные копии по расписанию	1. Изучить документацию и функционал системы (какие варианты настройки расписаний присутствуют)	Должны быть варианты автоматических бэкапов по календарю с указанием точного времени
	Выгрузка резервных копий на сторонний сервер	1. Изучить документацию и функционал системы (какие варианты выгрузки присуствуют, указать поддерживаемые протоколы)	Указать протоколы. Бэкапы должны выгружаться без ошибок и предупреждений

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		2. Сделать бэкап МСЭ и выгрузить его по одному из протоколов. 3. Сделать бэкап СУ и выгрузить его по одному из протоколов.	
	Восстановление из резервной копии NGFW	1. Сбросить МСЭ до заводских настроек. 2. Настроить минимальную конфигурацию для загрузки бэкапа и загрузить бэкап с сервера. 3. Восстановить систему из резервной копии	Устройство должно восстановить все настройки
	Восстановление из резервной копии Системы Управления	1. Сбросить СУ до заводских настроек (или удалить все политики и объекты). 2. Настроить минимальную конфигурацию для загрузки бэкапа и загрузить бэкап с сервера. 3. Восстановить систему из резервной копии	Устройство должно восстановить все настройки