МЕТОДИКА ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ УСТРОЙСТВ КЛАССА NGFW/UTM

JET SECURITY TEAM

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Базовые функции	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 INT (ETH2) 6. Настроить на тестовой рабочей станции в качестве шлюза по умолчанию INT (ETH2)-интерфейс тестируемого МСЭ 7. Проверить доступ к ресурсам интернет (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
	Работа в режиме L2 (Transparent Mode)	1. Выбрать режим функционирования L2 2. Настроить IP-адресацию MGMT-интерфейса и маршрут по умолчанию (при необходимости) Дальнейшие шаги могут отличаться в зависимости от тестируемого МСЭ, среды тестирования (vSphere, EVE-NG) и особенностей работы МСЭ в L2 3. Определить Internal/External-интерфейсы 4. Настроить правило доступа для разрешения трафика INT->EXT 5. Настроить на тестовой рабочей станции подключена в сегмент INT) в качестве шлюза по умолчанию интерфейс L3-устройства, являющийся шлюзом по умолчанию в сегменте EXT 6. Проверить доступ к внешним ресурсам/ресурсам интернет 7. Убедиться в наличии событий доступа с тестовой рабочей станции	1. Выход в интернет работает 2. События появляются в логах
	Режим получения динамических маршрутов при работе в кластере	1. Собрать и настроить кластер 2. Включить динамическую маршрутизацию	Проверить режимы получения динамических маршрутов. Ноды кластера должны успешно обмениваться динамическими маршрутами/Переключение кластера должно выполняться без перестройки процесса маршрутизации
	VRF	1. Создать и настроить VRF 2. Назначить интерфейсы указанным VRF	Пакеты должны правильно маршрутизироваться внутри соответствующих VRF
	Поведение МСЭ при ассиметричной маршрутизации	1. Передать трафик с использованием ассиметричных маршрутов 2. Выполнить изменение настроек МСЭ по обработке трафика при ассиметричной маршрутизации (при наличии такой возможности)	Зафиксировать поведение МСЭ при ассиметричной маршрутизации

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
	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	1. Создать несколько маршрутов с разными метриками 2. Передать трафик, который должен использовать эти маршруты	Пакеты должны использовать маршруты с более низкой/приоритетной метрикой
	Поддержка Fullview (маршрутизация)	1. Изучить документацию и функционал системы	МСЭ должен поддерживать Fullview
	ECMP	1. Настроить ECMP для определенных маршрутов 2. Передать трафик, который должен использовать ECMP	Пакеты должны равномерно распределяться между маршрутами в ECMP
	BFD	1. Настроить BFD для мониторинга состояния маршрутов	BFD должен корректно обнаруживать и реагировать на изменения 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
	VXLAN	1. Настроить и использовать VXLAN для передачи трафика	VXLAN должен быть успешно настроен и обеспечивать передачу трафика
	Резервирование канала	1. Настроить два канала 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	1. Настроить статическую балансировку для нескольких линков 2. Передать трафик через устройство и проверить распределение по линкам	Трафик должен быть равномерно распределен между линками в соответствии с настройками статической балансировки
	Динамическая балансировка трафика	1. Настроить динамическую балансировку 2. Имитировать изменение загруженности линков и проверить реакцию системы	Система должна динамически распределять трафик в соответствии с загруженностью линков
	Потери пакетов при выходе из строя одного линка при использовании LoadSharing Active/Active	1. Настроить Load Sharing Active/Active с несколькими линками 2. Отключить один из линков и передавать трафик	Потери пакетов должны быть минимальными при выходе из строя одного линка. Зафиксировать потери
	Механизмы мониторинга физических линков	1. Изучить документацию и функционал системы	Зафиксировать поддерживаемые механизмы мониторинга линков
	Работа ISP redundancy с VPN	1. Настроить ISP redundancy с VPN 2. Передать трафик через устройство и проверить работу VPN при смене ISP	VPN должен корректно работать при смене активного ISP
	Задание приоритета для линка	1. Установить различные приоритеты для линков 2. Передавать трафик и проверить соответствие приоритетам	Трафик должен предпочтительно передаваться через линки с более высоким приоритетом

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Базовые функции	Поддержка виртуальных контекстов	1. Настроить виртуальные контексты и передать трафик через них	Устройство должно корректно обрабатывать трафик в виртуальных контекстах
	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
	Fail Close/Fail Open (настройка поведения устройства при высокой нагрузке)	1. Настроить Fail Close и провести тест на срабатывание 2. Настроить Fail Open и провести тест на срабатывание	В режиме Fail Close система должна закрывать доступ при срабатывании условий, а в режиме Fail Open – оставлять доступ открытым
	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. Включить Netflow на устройстве 2. Настроить параметры Netflow 3. Передать трафик через устройство	Устройство должно начать генерировать Netflow-записи
	LACP	1. Настроить LACP для соединения с другим устройством 2. Передать трафик через LACP-канал	LACP-канал должен корректно обрабатывать трафик
	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 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
	Приоритизации Radius-серверов	1. Настроить несколько Radius-серверов с разными приоритетами 2. Передать запросы аутентификации через тестируемое устройство	Устройство должно использовать сервер с более высоким приоритетом при первоочередной попытке аутентификации
	ICAP Server	1. Настроить ICAP Server 2. Передать файл на проверку через ICAP	ICAP должен корректно проверить файл и вернуть результат
	ICAP Client	1. Настроить ICAP Client 2. Передать файл на проверку через ICAP	ICAP должен корректно проверить файл и вернуть результат
	Возможность поддержки ICAP без установки дополнительных модулей	1. Проверить возможность использования ICAP без установки дополнительных модулей на устройство	ICAP должен функционировать без необходимости установки дополнительных модулей
	Необходимость указывать VIP-адрес в качестве ICAP Server адреса на стороне клиентов при использовании VIP-адреса для кластера	1. Настроить ICAP Client с использованием VIP-адреса кластера 2. Передать файл на проверку через ICAP	МСЭ, работающий в качестве ICAP Server, должен для подключения клиента использовать VIP-адрес кластера
	QoS	1. Изучить документацию и функционал системы	Система должна поддерживать 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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Базовые функции	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
МСЭ (L4)	Использование зон безопасности в политиках ACL	**Проверка правил Allow** 1. Настроить правило доступа к ресурсам интернет, 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 ресурсам интернет, 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 ресурсам интернет, 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 Deny** 1. Настроить правило доступа, блокирующее доступ к ресурсам интернет, 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	**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
МСЭ (L4)	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Drap&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 трафика через NGFW	NGFW должен отслеживать состояние соединения и принимать решения на основе этой информации
	Ускорение обработки трафика	1. Узнать, какие механизмы ускорения обработки 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
	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 удалятся или отключатся
	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
МСЭ (L4)	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 блокировки по стране** Доступ должен быть заблокирован в соответствии с настройками GeoIP **Тест-кейс для исключения определенных IP**

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		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	**из блокировки** Доступ должен быть разрешен для исключенных IP, несмотря на блокировку GeoIP
NAT	Очередность выполнения NAT	1. Создать несколько правил NAT с разной очередностью выполнения 2. Передать трафик, соответствующий созданным правилам	NAT должен выполняться в порядке, установленном при создании правил, и результаты должны соответствовать ожиданиям
	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
	Bidirectional NAT	1. Создать Bidirectional NAT правило 2. Передать трафик, требующий применения Bidirectional NAT	Оба адреса (исходный и целевой) должны быть заменены в соответствии с правилом
	NAT inside 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
SSL INSPECTION	Поддерживаемые модули для SSL Inspection	1. Узнать, с какими модулями работает SSLIinspection	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	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
	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
SSL INSPECTION	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
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
	Создание кастомных сигнатур	1. Перейти в раздел создания сигнатур 2. Создать новую кастомную сигнатуру 3. Применить сигнатуру к трафику, содержащему соответствующий паттерн	Система должна успешно применять кастомную 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
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
Веб-фильтрация	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Ограничение используемых методов (GET, POST и др.) для отдельных URL-категорий	1. Ограничить использование определенных методов (GET, POST и т. д.) для выбранных URL-категорий 2. Передать трафик, используя ограниченные методы для URL из выбранной категории	Система должна блокировать трафик с использованием ограниченных методов
	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 принадлежность 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
BOTNET	Типы защищаемого трафика	**Тест-кейс для проверки работы с трафиком пользователей** 1. Передать трафик от разных пользователей через систему 2. Проверить, что система успешно обрабатывает и фильтрует трафик от каждого пользователя **Тест-кейс для проверки работы с защитой опубликованных серверов** 1. Направить трафик к опубликованным серверам 2. Проверить, что система обеспечивает защиту опубликованных серверов	**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. Передать трафик, содержащий признаки RAT 2. Проверить, что система успешно определяет и блокирует трафик, связанный с RAT	Система должна корректно идентифицировать и блокировать трафик от RAT
	Выявление обращений к вредоносными URL и доменам	1. Передать трафик, содержащий запросы к известным вредоносным URL и доменам 2. Проверить, что система успешно идентифицирует и блокирует такой трафик	Система должна корректно распознавать и блокировать трафик к вредоносным URL и доменам
BOTNET	Выявление IRC-коммуникаций	1. Передать трафик, содержащий IRC-коммуникации 2. Проверить, что система успешно распознает и блокирует IRC-коммуникации	Система должна корректно идентифицировать и блокировать трафик IRC-коммуникаций
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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	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
	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
	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 системы управления	Предоставлена информация о кластере системы управления
	Кластер системы централизованного логирования	1. Запросить информацию, как система обеспечивает кластер системы логирования	Предоставлена информация о кластере системы 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
SD-WAN	SD-WAN	1. Проверить наличие функционала SD-WAN в системе 2. Настроить и включить SD-WAN на устройстве	Система должна поддерживать SD-WAN, и функционал должен быть активирован и работоспособен
	Распределение пользователей (локальных и доменных) по каналам	1. Настроить политику SD-WAN для распределения пользователей локальных и AD по разным каналам	Трафик от пользователей локальных и AD должен быть успешно распределен по заданным каналам

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		2. Передать трафик от пользователей и проверить, что трафик распределяется в соответствии с настройками	
	Распределение трафика приложений/сайтов по каналам	1. Настроить политику SD-WAN для распределения трафика по определенным приложениям или сайтам в отдельные каналы 2. Передать трафик с использованием этих приложений или сайтов и проверить, что трафик направляется в соответствующие каналы	Трафик, связанный с указанными приложениями или сайтами, должен быть успешно направлен в соответствующие каналы
	Мониторинг трафика	1. Отправить трафик через систему 2. 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
	IPsec over SD-WAN	1. Настроить SD-WAN для обработки трафика IPsec 2. Передать трафик IPsec и проверить, что SD-WAN корректно обрабатывает этот трафик	SD-WAN должен успешно работать с трафиком IPsec, обеспечивая эффективное управление каналами
	Интеграция с модулями URL Filtering / Application Control	1. Настроить политику SD-WAN, используя категории сайтов/приложений из URL Filtering / Application Control 2. Передать трафик, включающий различные категории, и проверить, что SD-WAN правильно обрабатывает трафик в соответствии с настройками	SD-WAN должен успешно использовать категории сайтов/приложений из URL Filtering / Application Control в политиках
	Типы фильтров в политиках SD-WAN	1. Запросить информацию о типах фильтров в политиках SD-WAN	Предоставлена информация о типах фильтров
Логирование и отчёты	Модули с логированием	1. Запросить информацию о модулях с логированием	Предоставлена информация о модулях с логированием
	Выгрузка логов	1. Проверить наличие опции выгрузки логов 2. Выполнить выгрузку логов с устройства	Система должна предоставлять возможность выгрузки логов, и 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, и отправка логов должна быть успешной
	Типы отчеты	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, и логи должны быть соответствующим образом настроены
Логирование и отчёты	Виджеты для мониторинга трафика	1. Проверить наличие виджетов для мониторинга трафика в системе 2. Настроить виджеты для отображения конкретных данных о трафике	Система должна предоставлять виджеты для мониторинга трафика, и они должны корректно отображать выбранные данные
Защита почты	Защита почты	1. Проверить наличие функционала защиты почты в системе 2. Настроить и активировать функционал защиты почты	Система должна поддерживать функционал защиты почты, и он должен быть активирован

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	Поддерживаемые протоколы	1. Проверить поддерживаемые протоколы, такие как SMTP, POP3, IMAP 2. Передать почтовый трафик, используя различные протоколы, и убедиться, что защита почты работает корректно	Система должна поддерживать указанные протоколы для защиты почты, и защита почты должна эффективно работать
	Антиспам	1. Настроить и включить функционал антиспама 2. Передать трафик, содержащий спам и вирусы, и убедиться, что система успешно обнаруживает и блокирует подобный трафик	Функционал антиспама должен быть успешно настроен и активирован, и он должен эффективно блокировать соответствующий трафик
	Антивирусная проверка писем	1. Настроить и включить функционал антивируса 2. Передать трафик, содержащий спам и вирусы, и убедиться, что система успешно обнаруживает и блокирует подобный трафик	Функционал антивируса должен быть успешно настроен и активирован, и он должен эффективно блокировать соответствующий трафик
	MTA	1. Проверить поддержку функционала MTA (Mail Transfer Agent) 2. Передать почтовый трафик и убедиться, что MTA работает корректно	Система должна поддерживать функционал MTA, и он должен эффективно обрабатывать почтовый трафик
	DMARC/DKIM/SPF	1. Проверить поддержку стандартов DMARC, DKIM и SPF 2. Настроить эти стандарты для защиты почтового трафика	Система должна поддерживать стандарты DMARC, DKIM и SPF, и они должны успешно применяться для обеспечения безопасности почтового обмена
	Поддержка протоколов с шифрованием	1. Передать зашифрованный почтовый трафик (например, используя протокол TLS/SSL) 2. Убедиться, что система корректно обрабатывает зашифрованный трафик и применяет функционал защиты почты	Система должна поддерживать протоколы с поддержкой TLS/SSL для защиты почты, и защита почты должна эффективно работать
	Загрузка сторонних списков спам-сайтов	1. Попробовать загрузить свой собственный список спам-сайтов 2. Передать трафик, содержащий сайты из загруженного списка, и убедиться, что система успешно блокирует такие сайты	Система должна предоставлять возможность загрузки собственных списков спам-сайтов, и они должны успешно применяться для фильтрации трафика
Remote Access VPN	Поддерживаемые протоколы	1. Проверить список поддерживаемых протоколов VPN (например, IKEv1, IKEv2, SSL, TLS ГОСТ) 2. Убедиться, что система успешно устанавливает соединение с использованием каждого поддерживаемого протокола	Система должна поддерживать заявленные протоколы VPN, и каждый из них должен работать корректно
	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
Remote Access VPN	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	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	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 адрес отдельной ноды кластера
	ОС для клиента	1. Проверить список поддерживаемых операционных систем для клиента VPN 2. Убедиться, что клиент успешно устанавливается на каждой из поддерживаемых операционных систем	VPN-клиент должен успешно устанавливаться и работать на каждой из поддерживаемых операционных систем
	Способ получения клиента (ПО)	1. Проверить способы загрузки клиента для пользователя (например, с официального веб-сайта, через центр управления) 2. Убедиться, что загрузка клиента для пользователя происходит корректно	Способы загрузки клиента должны быть эффективными, и клиент должен успешно устанавливаться на устройство пользователя
	Автозапуск при включении ПК	1. Установить VPN-клиент 2. Перезагрузить устройство и проверить, запускается ли клиент автоматически	VPN-клиент должен иметь опцию автозапуска при включении устройства, и эта опция должна работать корректно
	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, где установлен VPN-клиент, должно успешно анализировать и обеспечивать безопасность VPN-трафика
	Централизованная установка клиента	1. Подготовить MSI-пакет для VPN-клиента 2. Развернуть MSI-пакет на нескольких устройствах и проверить успешность установки	Администратор должен успешно развернуть MSI-пакет на нескольких устройствах, и установка клиента должна быть успешной
Remote Access VPN	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
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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
	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 успешно видеть и 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
	Публикация портала на разных URL	1. Настроить портал для доступа по дополнительному URL 2. Попытаться открыть портал по этому дополнительному URL	Пользователь должен успешно получать доступ к порталу по дополнительному URL
	Поддержка 2FA	1. Включить настройку двухфакторной аутентификации на портале 2. Попытаться аутентифицироваться на портале, используя два фактора	Пользователь должен успешно аутентифицироваться, предоставив оба фактора
Site-to-Site VPN	Поддерживаемые протоколы	1. Проверить список поддерживаемых протоколов VPN (например, IKEv1, IKEv2, IPSec, TLS ГОСТ) 2. Убедиться, что система успешно устанавливает соединение с использованием каждого поддерживаемого протокола	Система должна поддерживать заявленные протоколы VPN, и каждый из них должен работать корректно
	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 неработающийbq 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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Site-to-Site VPN	SA lifetime	**Тест-кейс для проверки SA lifetime в режиме КБ** 1. Настроить SA lifetime в режиме, измеряемом в килобайтах 2. Проверить, что соединение устанавливается и поддерживается согласно установленному лимиту килобайт **Тест-кейс для проверки SA lifetime в режиме секунды/минуты** 1. Настроить SA lifetime в режиме, измеряемом в секундах или минутах 2. Проверить, что соединение устанавливается и поддерживается согласно установленному времени жизни	**Тест-кейс для проверки SA lifetime в режиме КБ** Система должна корректно устанавливать и поддерживать IPSEC соединение в соответствии с установленным лимитом по килобайтам **Тест-кейс для проверки SA lifetime в режиме секунды/минуты** Система должна корректно устанавливать и 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 на основании сервиса	1. Настроить VPN с исключением определенного сервиса из зашифрованного трафика 2. Проверить, что указанный сервис не проходит через VPN	Указанный сервис должен быть успешно исключен из VPN-трафика
	Алгоритмы шифрования	1. Проверить список поддерживаемых протоколов шифрования для Site-to-Site VPN	Система должна поддерживать различные протоколы шифрования, такие как AES, 3DES, ГОСТ и др.
	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
	IKEv1 Aggressive Mode	1. Настроить Site-to-Site VPN с использованием IKEv1 Aggressive Mode 2. Проверить успешность установки VPN-соединения	VPN-соединение должно успешно устанавливаться с использованием IKEv1 Aggressive Mode
	PFS (Perfect Forward Secrecy)	1. Включить PFS в настройках Site-to-Site VPN 2. Проверить, что новые ключи согласовываются с использованием PFS при переключении	PFS должно успешно работать, и 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
	GRE over IPSEC	1. Настроить Site-to-Site VPN с использованием протокола GRE внутри IPSEC 2. Проверить успешность установки и передачи трафика через GRE	GRE-трафик должен успешно проходить через IPSEC VPN
	IPSEC over GRE	1. Настроить Site-to-Site VPN с использованием IPSEC внутри протокола GRE 2. Проверить успешность установки и передачи трафика через IPSEC over GRE	IPSEC-трафик должен успешно проходить через GRE VPN
	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
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 запрета загрузки файлов 2. Попытаться загрузить файлы различных типов	Файлы должны быть успешно загруженызаблокированы в соответствии с установленными фильтрами
	Запрет отправки файлов	1. Настроить фильтры для запретаконтроля выгрузки отправки файлов 2. Попытаться выгрузить отправить файлы различных типов	Файлы должны быть успешно выгруженызаблокированы в соответствии с установленными фильтрами
2FA	2FA + Remote Access VPN с клиентом	**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	**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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
2FA	2FA + Remote Access VPN с SSL-порталом	**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 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	**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 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
Централизованное управление	Выделенный сервер управления	1. Проверить документацию и конфигурацию системы	Должен быть выделенный сервер управления, если он предусмотрен системой
	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
	Кластер сервера управления	1. Настроить кластеризацию на Центре управления 2. Изменить конфигурацию или политику на одном из серверов и проверить изменения на другом	Изменения, внесенные на одном сервере, должны быть отражены на другом из-за кластеризации
	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 логирование	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Централизованное логирование	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
	Регистрация и управление зарегистрированными инцидентами	1. Изучить документацию и функционал системы	Система должна предоставлять функционал для регистрации и управления инцидентами
Proxy (explicit/transparent)	Explicit Proxy	1. Настроить явный прокси в системе 2. Перенаправить трафик через явный прокси	Проксирование должно быть успешно выполнено, и трафик должен проходить через явный прокси
	Transparent Proxy	1. Настроить прозрачный прокси в системе 2. Перенаправить трафик через прозрачный прокси	Прозрачное проксирование должно быть успешно выполнено, и трафик должен проходить через прозрачный прокси
	Модули, работающие вместе с HTTPS Proxy	1. Активировать HTTPS Proxy 2. Проверить, какие модули работают с HTTPS Proxy (например, Web Filter, URL Filtering)	Модули должны успешно взаимодействовать с HTTPS Proxy, обеспечивая безопасность и фильтрацию трафика
	Авторизация Kerberos	1. Настроить авторизацию через Kerberos 2. Попытаться получить доступ с использованием Kerberos-авторизации	Авторизация через Kerberos должна быть успешной
	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
Траблшутинг	Модули диагностики в GUI	1. Проверить раздел «Troubleshooting» в GUI для доступных модулей	Должны 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 версии ПО	Обновление кластера	1. Выполнить обновление кластера в соответствии с документацией вендора	Обновление должно проходить успешно.
	Обновление кластера без простоя	1. Выполнить обновление кластера в соответствии с документацией вендора.	Обновление должно проходить без простоя
	Резервное копирование при автоматическом обновлении	1. Проверить, происходит ли автоматическое создание резервной копии перед обновлением	Автоматическая резервная копия должна быть создана
	Возможность отката к предыдущей версии	1. Попытаться выполнить откат к предыдущей версии	Откат должен быть возможен

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Обновление версии ПО	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
	Оффлайн-обновления	1. Попытаться выполнить обновление без доступа к интернету	Должна быть предусмотрена возможность оффлайн-обновлений, либо процесс должен предоставить необходимые инструкции для оффлайн-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
Обновление лицензии	Оффлайн-установка лицензии (без доступа в интернет)	1. Попытаться установить лицензию без подключения к интернету	Должна быть предоставлена возможность установить лицензию без подключения к интернету
Защита от DoS	Защита от DoS	1. Проверить наличие и функциональность DoS-защиты	Должна быть поддержка и корректная работа средств защиты от DoS-атак
	Функционал защиты от DoS в правилах IPS	1. Проверить, есть ли функционал защиты от DoS в правилах IPS	Должен быть указан функционал защиты от DoS в правилах IPS, если отдельного модуля для защиты от DoS нет
PBR (Policy Based Routing)	PBR	1. Проверить наличие и функциональность PBR	Должна быть поддержка и корректная работа PBR
	Отказоустойчивый линк 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
	Совместная работа с GRE	1. Настроить PBR с использованием GRE 2. Переслать трафик через GRE-интерфейс	PBR должен корректно обрабатывать трафик через GRE, без сбоев
	Совместная работа с Route-based VPN	1. Настроить Route-based VPN 2. Применить PBR к трафику VPN	PBR должен взаимодействовать корректно с Route-based VPN, обеспечивая правильное маршрутизирование трафика
Наличие API или других инструментов для миграции правил	API	1. Проверить наличие и функциональность API	Должно быть подтверждено наличие API с подробной документацией
	Модули, доступные через API	1. Выбрать правила для миграции 2. Использовать инструменты миграции, указанные в документации	Правила должны быть успешно мигрированы согласно указанным инструкциям и инструментам
	Загрузка политик через web-интерфейс	1. Загрузить конфигурацию политик через веб-интерфейс	Конфигурация политик должна быть успешно загружена без ошибок
	Загрузка политик через CLI	1. Загрузить конфигурацию политик через командную строку	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
	Требуется ли установка стороннего ПО для модернизации политик/скрипта	1. Проверить в документации и инструкциях наличие требований к стороннему софту для миграции политик	Должны быть четкие указания о необходимости или отсутствии стороннего софта для успешной миграции политик

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Межсетевое экранирование (L7 - Application Control)	Ограничение трафика пользователя или группы пользователей в нерабочее или обеденное время	1. Настроить политику ограничения трафика для конкретного пользователя в нерабочее/обеденное время 2. Попробовать доступ в разные часы	Доступ к ресурсам ограничен в указанные периоды
	Ограничение трафика IP-адресу или группе IP-адресов в нерабочее или обеденное время	1. Настроить политику ограничения трафика для конкретного IP-адреса в нерабочее/обеденное время 2. Попробовать доступ в разные часы	Доступ к ресурсам ограничен в указанные периоды
	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» 2. Попробовать выход на запрещенный сайт 3. Заполнить форму	Администратор должен получить заполненную форму, и пользователь должен продолжить работу после предупреждения
	Блокировка QUIC-протокола	1. Настроить политику блокировки протокола QUIC 2. Протестировать трафик, использующий протокол QUIC	Трафик, использующий протокол QUIC, должен быть успешно заблокирован
Antivirus	Проверка почтового трафика SMTP(S), POP3, IMAP	1. Отправить тестовые письма с вложениями через SMTP 2. Проверить письма через POP3 и IMAP	Антивирус должен успешно сканировать и блокировать вредоносные вложения
	Использование сторонних сигнатур Threat Feed	1. Подключить сторонний Threat Feed к антивирусному модулю 2. Запустить тестовый трафик с вирусами, известными Threat Feed	Антивирус должен успешно использовать сторонние сигнатуры для обнаружения вирусов
	Страница блокировки сайта в случае наличия вируса на странице (URL-категория)	1. Посетить вредоносный сайт	Должна появиться страница блокировки с информацией о наличии вируса
	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

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Antivirus	Проверка FTP, SFTP, SCP	1. Передать вредоносный файл по протоколам FTP, SFTP, SCP	Антивирус должен успешно обнаруживать и блокировать вредоносные файлы
	Проверка SMB	1. Передать вредоносный файл по протоколу SMB	Антивирус должен успешно обнаруживать и блокировать вредоносные файлы
	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. Создать собственные сигнатуры для антивируса 2. Передать файлы, соответствующие созданным сигнатурам	Антивирус должен успешно обнаруживать и блокировать файлы с использованием созданных сигнатур
Интеграция с 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 Заметках 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
	Требования к ПО для LDAP-аутентификации	1. Изучить документацию и функционал системы	Зафиксировать требования к дополнительному ПО для LDAP-аутентификации
	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. Настроить Kerberos, используя LDAP	Функционал должен быть успешно настроен с использованием данных из LDAP
	Proxy-аутентификация	1. Настроить Proxy-аутентификацию, используя LDAP	Функционал должен быть успешно настроен с использованием данных из LDAP
	Прозрачная аутентификация	1. Настроить прозрачную аутентификацию, используя LDAP	Функционал должен быть успешно настроен с использованием данных из LDAP
	Версия ОС LDAP-сервера	1. Изучить документацию и функционал системы	Зафиксировать поддерживаемые ОС LDAP-серверов
	Secure LDAP	1. Настроить защищенное соединение с LDAP на порту 636	Защищенное соединение должно быть успешно настроено и работать

Инфосистемы Джет

+7 495 411 76 01 | security@jet.su

jet.su

JET SECURITY TEAM

Jet