Инфосистемы Джет

ПОЛНЫЕ РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

ОГЛАВЛЕНИЕ

О ПРОЕКТЕ

Основная цель — дать наиболее полное представление о доступных в России решениях класса NGFW и их функциональных возможностях.

Наша задача — по единой методологии проверить, как функционируют различные устройства в условиях, максимально приближенных к реальным. Мы рекомендуем рассматривать представленные результаты как отправную точку при выборе решения для дальнейшего проведения пилотных тестов в вашей организации.

Следите за обновлениями на сайте: https://jet.su/ngfw/

МЕТОДИКА

Испытание прошло в режиме, в котором чаще всего используется NGFW у наших клиентов: периметровый межсетевой экран с включенными модулями IPS, антивирус, контентная фильтрация, контроль приложений, SSL Inspection, VPN и Proxy.

В рамках нагрузочного тестирования мы взяли за основу типичные настройки для организации с количеством сотрудников от 500 до 1000 человек, наличием 1-2 филиалов и использованием таких корпоративных приложений, как почта, CRM, аудио- и видеоконференцсвязь, корпоративный портал.

МЕТОДИКА НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ В .PDF
МЕТОДИКА ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ В .PDF

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Сетевые функции									
Режимы работы	1.1	Работа в режиме L3 (Routing Mode)	Да	Да	Да	Да	Да	Да	Да
	1.2	Работа в режиме L2 (Transparent Mode)	Нет	Да	Да	Да	Нет	Нет	Да
Маршрутизация	1.3	Режим получения динамических маршрутов при работе в кластере	Активная нода	Обе ноды	Обе ноды	При использовании OSPF маршруты получает активная нода и синхронизирует их с пассивной нодой	Маршруты получает активная нода. При переключении кластера пассивная нода получает маршруты	Активная нода	Нет
	1.4	Поведение МСЭ при ассиметричной маршрутизации	Трафик блокируется	В зависимости от настроек	В зависимости от настроек	Трафик блокируется	Трафик блокируется	Трафик блокируется	Нет
	1.5	Возможность указывать исходящий интерфейс при настройке маршрутизации	Да, с ограничениями	Да	Да	Да	Да, с ограничениями	Нет	Да
	1.6	Приоритизация маршрутов	Да	Да	Да	Да	Да	Да	Да
	1.7	Поддержка Fullview (маршрутизация)	Да, с ограничениями	Да	Да	Не тестировалось	Да	Нет	Да
	1.8	ECMP	Да	Да	Да	Да	Да, с ограничениями	Да	Да
	1.9	BFD	Нет	Да	Да	Да	Да, с ограничениями	Нет	Да
	1.10	Протоколы маршрутизации	OSPF, BGP	RIP, OSPF, BGP, IS-IS, PIM	OSPF, BGP, RIP, PIM	RIP, OSPF, BGP	OSPF, BGP	OSPF, BGP	RIP, OSPF, BGP, IS-IS, PIM

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Сетевые функции									
Маршрутизация	1.11	Ограничения для поддерживаемых динамических протоколов	В ходе тестирования ограничений не выявлено	В ходе тестирования ограничений не выявлено	Нет редистрибуции из BGP в OSPF	Max BGP members 128	Ограниченная настройка через web, отсутствие loopback. Планируются улучшения в версии 18	Для OSPF: 1. Можно указать не более 128 сетей, в которых осуществляется обмен информацией по протоколу OSPF. 2. На каждом интерфейсе можно создать не более 255 ключей с уникальным keyid и только один пароль.	Не обнаружено в ходе тестирования
Интерфейсы	1.12	VXLAN	Нет	Да	Да	Да	Нет	Нет	Да
	1.13	LACP	Да	Да	Да	Да	Да	Да	Да
Внешние каналы	1.14	Резервирование канала	Да	Да	Да	Да	Да	Да	Да
	1.15	Сколько ISP поддерживается	По количеству физических интерфейсов	До 10	Без ограничений	Без ограничений	По количеству физических интерфейсов	По количеству физических интерфейсов	По количеству физических интерфейсов
	1.16	Статическая балансировка трафика	Да	Да	Да	Да	Да	Да	Да
	1.17	Динамическая балансировка трафика	Да	Да	Нет	Нет	Да	Да	Да
	1.18	Механизмы мониторинга физических линков	ICMP Probing	ICMP Probing, HTTP Request (SD-WAN)	Link up\down	BDF, ICMP, ARP, DNS	ICMP, Round-Robin	Используется проверка состояния шлюзов (Dead Gateway Detection, DGD)	ICMP, TTL-тест, пользовательский скрипт
	1.19	Работа ISP redundancy с VPN	Да, с ограничениями	Да	Да	Да	Да	Да	Да
	1.20	Задание приоритета для линка	Да	Да	Да	Да	Да	Да	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Сетевые функции									
Базовые функции	1.21	Поддержка виртуальных контекстов	Нет	Да	Нет	Да	Нет	Нет	Нет
	1.22	VRF	Нет	Да, с ограничениями	Да	Да	Нет	Нет	Да
	1.23	Настройка Proxy ARP	Ручная настройка	Ручная настройка	Ручная настройка	Ручная настройка	Proxy ARP включен по умолчанию, изменить нельзя	Нет	Ручная настройка
	1.24	Fail Close/Fail Open (настройка поведения устройства при высокой нагрузке)	Да	Да	Нет	Да	Нет	Нет	Нет
	1.25	Поведение устройства при обновлении правил/применении политики	В зависимости от настроек: разрывает сессии или сохраняет текущие сессии	Устройство продолжает обрабатывать трафик, сессии не разрываются	В зависимости от настроек: разрывает сессии или сохраняет текущие сессии	Повторное сравнение согласно новой политике. Устройство продолжает обрабатывать трафик, сессии не разрываются	Устройство продолжает обрабатывать трафик, сессии не разрываются	Правила/политики применяются без перерывов в обслуживании	Устройство продолжает обрабатывать трафик, сессии не разрываются
	1.26	Netflow	Да	Да	Да	Нет	Нет	Нет	Да
QoS	1.27	QoS	Да	Да	Да	Да	Да	Да	Да
	1.28	Применение QoS политик отдельно для интерфейсов	Да	Да	Нет	Да, с ограничениями	Да, с ограничениями	Нет	Да
	1.29	Применение QoS политик для зон (zones)	Нет	Да	Да	Нет	Да, с ограничениями	Нет	Нет
Функции МСЭ									
МСЭ (L4)	2.1	Использование зон безопасности в политиках ACL	Нет	Да	Да	Да	Да	Да	Да
	2.2	Использование интерфейсов в политиках ACL	Да, с ограничениями	Да	Да, с ограничениями	Да, с ограничениями	Да	Да	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции МСЭ									
МСЭ (L4)	2.3	Возможность включения интерфейсов в зоны	Нет	Да	Да	Да	Да	Да	Да
	2.4	Drag&Drop при работе с объектами и политиками	Да	Да	Да	Да	Нет	Да, с ограничениями	Нет
	2.5	Stateful Inspection	Да	Да	Да	Да	Да	Да	Да
	2.6	Ускорение обработки трафика	Да	Да	Нет	Да	Нет	Да	Да
	2.7	NAT-правила для определенных правил МСЭ	Да	Нет	Нет	Нет	Нет	Нет	Нет
	2.8	Расписание действия правил МСЭ	Да	Да	Да	Да	Да	Да	Да
	2.9	Поддержка временных правил МСЭ	Нет	Да	Да	Нет	Нет	Нет	Да
	2.10	Просмотр Implicit-правил	Да, с ограничениями	Да	Да	Да	Да, с ограничениями	Да	Нет
	2.11	Управление Implicit-правилами	Нет	Да	Нет	Да	Нет	Нет	Нет
	2.12	Hit Count для каждого правила	Нет	Да	Да	Да	Да	Да	Да
	2.13	Поиск правил по объекту	Да	Да	Да, с ограничениями	Да	Да	Да, с ограничениями	Нет
	2.14	Проверка правил на дубликаты	Нет	Да	Нет	Да	Нет	Да, с ограничениями	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции МСЭ									
МСЭ (L4)	2.15	Объекты для создания правил	IP host, IP range, IP-сеть, Сервисы и порты, Протоколы, Приложения, Группы, Страны, Пользователи (локальные и доменные)	Network, Host, Service, Application, VPN, User, Servers, Time Objects, Limit, Updatable Objects, Network Feed, Dynamic objects, DC Objects, Domain	Зона, Адрес источника, Список адресов, Список GeoIP, Список доменов, Пользователь, Группа пользователей	Source Zone, Source Address, User/Group, Destination Address, Service, Applications/Groups	IP host, IP range, Пользовательские группы, Сервисы и порты, Протоколы, Типы приложений, Домен, Список стран	IP host, IP range, IP network, DNS-имена, Интерфейсы и Группы интерфейсов, Сервисы и порты, Прикладные протоколы, Пользователи, Приложения и Группы приложений	IP host, group IP, ports, group ports, interfaces, group interfaces, networks, group networks, protocols
	2.16	Блокировка по GeoIP	Да	Да	Да	Да	Да	Нет	Нет
NAT	2.17	Очередность выполнения NAT	Используется политика NAT. Правила обрабатываются по порядку сверху вниз, правила DNAT имеют приоритет	Manual Static NAT (Port Forwarding, Bi-directional NAT) -> Automatic Static NAT -> Hide NAT	По каждому типу правил правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нем условия	По порядку написания в политике NAT	1. SNAT. 2. DNAT	По порядку размещения правил NAT, сверху вниз	По порядку размещения правил NAT, сверху вниз
	2.18	Возможность выбора интерфейса, на котором будет осуществляться NAT	Да	Нет	Да, с ограничениями	Да	Да	Нет	Да
	2.19	Source NAT	Да	Да	Да	Да	Да	Да	Да
	2.20	Destination NAT	Да	Да	Да	Да	Да	Да	Да
	2.21	Bidirectional NAT	Да	Да	Да	Да	Да	Да	Да
	2.22	NAT inside VPN	Да	Да	Да	Да	Да	Да	Да
PBR (Policy Based Routing)	2.23	PBR	Да	Да	Да	Да	Да	Да	Да
	2.24	Отказоустойчивый линк с провайдером при использовании PBR	Да	Да	Нет	Да	Да	Да	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции МСЭ									
PBR (Policy Based Routing)	2.25	Совместная работа с GRE	Нет	Да	Да	Да	Нет	Нет	Да
	2.26	Совместная работа с Route-based VPN	Нет	Да	Нет	Да	Да	Да	Да
Функции NGFW/UTM									
IPS	3.1	IPS	Да	Да	Да	Да	Да	Да	Да
	3.2	Возможность выбора определенной группы сигнатур для защиты	Да	Да	Да	Да	Нет	Да	Нет
	3.3	Создание исключений	Да	Да	Да	Да	Да	Да, с ограничениями	Нет
	3.4	Создание кастомных сигнатур	Да	Да	Да	Да	Да	Нет	Да
	3.5	Наличие документации, описывающей синтаксис, используемый при написании сигнатуры	Да	Да	Да	Да	Да	Нет	Да
Защита от DoS	3.6	Защита от DoS	Да	Да	Да	Да	Да	Да, с ограничениями	Да
	3.7	Функционал защиты от DoS в правилах IPS	Да	Да	Да	Да	Да	Да	Да
Application Control	3.8	Ограничение трафика пользователя или группы пользователей в нерабочее или обеденное время	Да	Да	Да	Да	Да	Да	Нет
	3.9	Ограничение трафика IP-адресу или группе IP-адресов в нерабочее или обеденное время	Да	Да	Да	Да	Да	Да	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
Application Control	3.10	Поддержка сложных правил. Например: 1. Разрешить трафик на YouTube, но запретить оставлять комментарии 2. Разрешить трафик VK, но запретить пользоваться Multimedia	Да	Да	Да, с ограничениями	Да, с ограничениями	Да, с ограничениями	Нет	Нет
	3.11	Добавление собственных приложений	Да, с ограничениями	Да	Да	Да	Нет	Нет	Нет
	3.12	Конфигурация сервисов на определенных портах	Да	Да	Да	Да	Нет	Да	Нет
	3.13	Политика реализации Application Control	Blacklist, Whitelist	Blacklist, Whitelist	Blacklist	Blacklist, Whitelist	Blacklist, Whitelist	Whitelist	Нет
	3.14	Политика для трафика — «Неизвестный или не мог быть опознан устройством»	Определяется последующим правилом для данного трафика	Accept, Deny (Drop)	Разрешить, Запретить	Нет	Неопознанный трафик в модуле Контент-фильтрация	Определяется последующим правилом для данного трафика	Нет
	3.15	Страница оповещения для пользователя (блокировка)	Да, с ограничениями	Да	Да	Да	Нет	Нет	Нет
	3.16	Страница оповещения для пользователя (предупредить и продолжить)	Нет	Да	Да	Нет	Нет	Нет	Нет
	3.17	Блокировка QUIC-протокола	Да	Да	Да	Да	Да	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
Antivirus	3.18	Проверка почтового трафика SMTP(S), POP3, IMAP	Нет	Да	Да	Да	Да, с ограничениями	Нет	Нет
	3.19	Использование сторонних сигнатур Threat Feed	Да	Пользовательские и внешние источники в форматах STIX XML (STIX 1.0), CSV в формате Check Point, CSV в других форматах	Да	Нет	Нет	Нет	Нет
	3.20	Страница блокировки сайта в случае наличия вируса на странице (URL-категория)	Да	Да	Да	Да	Да	Нет	Нет
	3.21	Условия работы антивируса	Проверка только трафика инспектируемого SSL Inspection, протоколы HTTP и HTTPS	Нет дополнительных условий	Нет	Нет дополнительных условий	ClamAV — без дополнительных условий. Kaspersky — при активации дополнительной лицензии	Нет	Нет
	3.22	Проверка скачиваемых файлов	Да	Да	Да	Да	Да	Нет	Нет
	3.23	Проверка FTP, SFTP, SCP	Нет	Да	Нет	Да, с ограничениями	Нет	Нет	Нет
	3.24	Проверка SMB	Нет	Да	Нет	Да	Нет	Нет	Нет
	3.25	Типы файлов	Более 40 типов файлов	Более 90 типов файлов	По типам файлов не дифференцируется. Проверяется hash файлов	Более 100 типов файлов, можно редактировать	Зависит от выбранного антивируса. Поддерживается более 90 типов файлов	Нет	Нет
	3.26	Проверка файлов в архивах без паролей	Да	Да	Да	Да	Да	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
Antivirus	3.27	Проверка файлов в архивах с паролями	Нет	Да	Нет	Нет	Нет	Нет	Нет
	3.28	Выбор действий для определенных типов файлов	Да	Да	Нет	Да	Нет	Нет	Нет
	3.29	Антивирусный движок	Проверка по хешам	Check Point Propreitary	Проприетарный	Собственный	Kaspersky, ClamAV	Нет	Нет
	3.30	Поддержка добавления пользовательских хешей	Да	Да	Да	Нет	Нет	Нет	Нет
SSL Inspection	3.31	Поддерживаемые модули для SSL Inspection	Антивирус, WEB-категоризация, Feeds, ICAP Client	FW, IPS, Application Control, URL filtering, AV, Sandbox	Контентная фильтрация, IPS, AppControl	Все модули	Контентная фильтрация, Антивирус, ICAP	Нет	Нет
	3.32	Поддерживаемые протоколы	HTTPS	SSH, SMTPS, HTTPS	HTTPS, SMTPS, POP3	HTTPS	HTTPS	Нет	Нет
	3.33	Поддержка нестандартных портов для поддерживаемых протоколов	Да	Да	Нет	Да, с ограничениями	Нет	Нет	Нет
	3.34	Возможность использовать сертификаты стороннего УЦ	Нет	Да	Да	Да	Да	Нет	Нет
	3.35	Инспектирование для отдельных пользователей	Да	Да	Да	Нет	Да	Нет	Нет
	3.36	Инспектирование для отдельных сайтов	Да	Да	Да	Да	Да	Нет	Нет
	3.37	Поддержка Wildcard-сертификатов	Да	Да	Да	Да	Да	Нет	Нет
	3.38	Client-Side (Outbound SSL Inspection)	Да	Да	Да	Да	Да	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
SSL Inspection	3.39	Server-Side (Inbound SSL Inspection)	Нет	Да	Да	Да	Нет	Нет	Нет
Веб-фильтрация	3.40	Использование собственных или сторонних списков URL	Да, обновление в ручном или автоматическом режимах	Да, обновление в ручном или автоматическом режимах	Да, обновление в ручном или автоматическом режимах	Да, обновление в ручном режиме	Можно загружать собственный список. Неудобный формат ввода в виде одной строчки, но используется автоматический парсинг данной строки	Загрузка списков URL не поддерживается, можно создавать группы объектов, добавляя каждый URL вручную	Да, обновление в ручном или автоматическом режиме
	3.41	Тип используемой базы URL	Локальная	Локальная	Локальная	Локальная	Локальная база (обновляемая)	Локальная, используется в модуле Контроль приложений	Онлайн обновление
	3.42	Создание кастомных URL-категорий	Да	Да	Да	Да	Да	Нет	Нет
	3.43	Переопределение категории URL	Да, с ограничениями	Да	Да	Да	Да, с ограничениями	Нет	Нет
	3.44	Ограничение используемых методов (GET, POST и др.) для отдельных URL-категорий	Да	Да	Да	Да	Нет	Нет	Нет
	3.45	Настройка доступа к определенным URL/доменам	Да	Да	Да	Да	Да	Да	Да
	3.46	URL Lookup (проверка принадлежность URL к определенной категории)	Нет	Да	Да	Да	Да	Нет	Нет
	3.47	Страница блокировки/ предупреждения	Да	Да	Да	Да	Да	Нет	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
Веб-фильтрация	3.48	Какие списки URL использует производитель	SkyDNS, TI feeds (Kaspersky, КБ, ЦБ)	Check Point Threat Cloud, Extermal Threat Feed	Собственные списки производителя	Собственные списки производителя	SkyDNS	Собственные	Open Source
Proxy (explicit/transparent)	3.49	Explicit Proxy	Нет	Да	Да	Нет	Да	Да	Да
	3.50	Transparent Proxy	Да	Да	Да	Да	Да	Да	Нет
	3.51	Модули, работающие вместе с HTTPS Proxy	Антивирус, TI Feeds, Категоризация сайтов, ICAP-client, Авторизация пользователей	Все модули Threat Prevention	Контентная фильтрация, IPS, AppControl	Нет	Контентная фильтрация, Антивирус, ICAP	Нет	URL Filtering
	3.52	Авторизация Kerberos	Да	Да	Да	Нет	Да	Нет	Да
	3.53	Страница блокировки на Captive Portal	Да	Да	Да	Да	Да	Да	Да
	3.54	Captive Portal для авторизации на Proxy	Да	Да	Да	Да	Да	Да	Нет
Content Filtering	3.55	Контентная фильтрация	Да	Да	Да	Да	Да	Да	Нет
	3.56	Типы файлов для фильтрации	Больше 40 категорий, блокируемых по расширениям и MIME-type. Предустановленные группы файлов (Исполняемые файлы, Архивы, Видеофайлы, Аудиофайлы, Flash-видео, Active-X, Torrent-файлы, Документы). Работа по фильтрации HTTPS-трафика по данному типу категорий возможна только при его расшифровке	Более 80 типов файлов	Видео, документы, звуки и музыка, картинки, приложения, JS	Более 100 типов файлов, можно редактировать	Аудиофайлы, Видеофайлы, Документы, Архивы, Torrent-файлы, Flash-видео, исполняемые файлы	Более 95 типов файлов	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
Content Filtering	3.57	Блокировка файлов в архивах	Нет	Да	Нет	Да	Нет	Да	Нет
	3.58	Блокировка архивов внутри архивов	Да	Да	Нет	Да	Нет	Нет	Нет
	3.59	Запрет загрузки файлов	Да	Да	Да	Да	Да	Да, с ограничениями	Нет
	3.60	Запрет отправки файлов	Да	Да	Да	Да	Да, с ограничениями	Нет	Нет
Anti Bot	3.61	Типы защищаемого трафика	Пользовательский трафик, трафик опубликованных серверов	Пользовательский трафик, трафик опубликованных серверов	Пользовательский трафик, трафик опубликованных серверов	Пользовательский трафик, трафик опубликованных серверов	Пользовательский трафик, трафик опубликованных серверов	Пользовательский трафик, трафик опубликованных серверов. Защита от Botnet реализована в модуле IPS	Нет
	3.62	Частота обновлений	Динамично: от нескольких раз в день до нескольких раз в неделю	Возможна ручная конфигурация (до 1 раза в час)	Раз в неделю	База вендора обновляется по мере выявления новых угроз. База на МСЭ обновляется по настраиваемому расписанию	Несколько раз в день	Один раз в день	Нет
	3.63	Место хранения баз	Загружаются с сервера обновлений, хранятся локально на ЦУС	Локально	Локально	Локально	Локальная база (обновляемая)	Локально	Нет
	3.64	Выявление трафика RAT	Да	Да	Нет	Да	Да	Да, с ограничениями	Нет
	3.65	Выявление обращений к вредоносными URL и доменам	Да	Да	Да	Да	Да	Да, с ограничениями	Нет
	3.66	Выявление IRC-коммуникаций	Нет	Да	Да, с ограничениями	Нет	Да	Да, с ограничениями	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Функции NGFW/UTM									
Защита почтового трафика	3.67	Защита почты	Нет	Да	Да	Да	Да	Нет	Нет
	3.68	Поддерживаемые протоколы	Нет	SMTP, POP3, IMAP	POP3 и SMTP	SMTP, POP3, IMAP	IMAP(S), POP3(S)	Нет	Нет
	3.69	Антиспам	Нет	Да	Да	Нет	Да	Нет	Нет
	3.70	Антивирусная проверка писем	Нет	Да	Да	Да	Да, с ограничениями	Нет	Нет
	3.71	MTA	Нет	Да	Нет	Нет	Да	Нет	Нет
	3.72	DMARC/DKIM/SPF	Нет	Да	Нет	Нет	Да, с ограничениями	Нет	Нет
	3.73	Поддержка протоколов с шифрованием	Нет	Да	Да	Нет	Да	Нет	Нет
	3.74	Загрузка сторонних списков спам-сайтов	Нет	Да	Да	Нет	Нет	Нет	Нет
VPN и SD-WAN									
Remote Access VPN	4.1	Поддерживаемые протоколы	TLS ГОСТ	IKEv1, IKEv2, IPSec, L2TP	L2TP over IPSec, IKEv2 с PSK, IKEv2 с сертификатом	SSL VPN	PPTP, PPPoE, IKEv2/IPsec, SSTP, L2TP/IPsec, Wireguard	IPlir	WireGuard, IPsec, OpenVPN, OpenConnect
	4.2	Интеграция с LDAP	Да	Да	Да	Да	Да	Нет	Нет
	4.3	VPN-клиент	Да	Да	Да	Да	Да	Да	Нет
	4.4	Автоматическое назначение IP-адреса клиенту	Да	Да	Да	Да	Да	Да, с ограничениями	Да
	4.5	Поддержка 2FA	Да	Да	Да	Да	Да	Да	Нет
	4.6	Получение маршрутов от шлюза	Да	Да	Да	Да	Да	Да	Да
	4.7	SPLIT Tunnel	Да	Да	Нет	Да	Да	Нет	Нет
	4.8	Направление всего трафика через VPN	Да	Да	Да	Нет	Да	Да	Нет
	4.9	Подключение к VIP-адресу кластера шлюзов	Да	Да	Да	Да	Да	Да	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
VPN и SD-WAN									
Remote Access VPN	4.10	ОС для клиента	Windows, Linux, Android, iOS, MacOS, Аврора	Windows, Linux, Android, iOS, MacOS	Windows 8/10	Windows, Linux, MacOS, Android, iOS	Windows. MAC OS планируется в версии 17. Linux планируется в версии 18	Linux, Windows, Android, iOS, MacOS, Аврора	Нет
	4.11	Способ получения клиента (ПО)	Через дистрибутив или сайт	Сайт поддержки, портал SSL VPN	Через дистрибутив	SSL VPN портал, ТП вендора	Через дистрибутив или личный кабинет пользователя на Ideco NGFW	Сайт вендора, поставка на CD	Нет
	4.12	Автозапуск при включении ПК	Да	Да	Да, с ограничениями	Да	Да	Да	Нет
	4.13	Проверка трафика на шлюзе	Да	Да	Да	Да	Да	Да	Да
	4.14	Проверка трафика на клиентском устройстве	Нет	Да	Да	Нет	Да	Да, с ограничениями	Да
	4.15	Compliance Check клиента	Да	Да	Нет	Нет	Нет	Да	Нет
	4.16	Централизованная установка клиента	Нет	Да	Да	Нет	Да	Да	Нет
	4.17	Алгоритмы шифрования	ГОСТ	DES, 3DES, AES-128, AES-256	AES	DES, 3DES, AES/AES128, AES192, AES256, проприетарный_DES	AES256-GCM, AES256	ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018	aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, aes128ccm64, aes192ccm64, aes256ccm64, aes128ccm96, aes192ccm96, aes256ccm96, aes128ccm128, aes192ccm128, aes256ccm128, aes128gcm64, aes192gcm64,

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ									
ГРУППА ФУНКЦИОНАЛА	**№ П/П**	**КЕЙС**	**КОНТИНЕНТ 4.1.7**	**CHECKPOINT R81.20**	**USERGATE 7.1.0**	**РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0**	**IDECO NGFW V16**	**VIPNET COORDINATOR HW5 5.3**	**INFOWATCH ARMA СТЕНА (NGFW)**
									aes256gcm64, aes128gcm96, aes192gcm96, aes256gcm96, aes128gcm128, aes192gcm128, aes256gcm128, aes128gmac, aes192gmac, aes256gmac, 3des, blowfish128, blowfish192, blowfish256, camellia128, camellia192, camellia256, camellia128ctr, camellia192ctr, camellia256ctr, camellia128ccm64, camellia192ccm64, camellia256ccm64, camellia128ccm96, camellia192ccm96, camellia256ccm96, camellia128ccm128, camellia192ccm128, camellia256ccm128, serpent128, serpent192, serpent256, twofish128, twofish192, twofish256, cast128, chacha20poly1305, des, bf128, bf256, aes128gcm, aes192gcm, aes256gcm, TLS
WEB-portal VPN	4.18	Кастомизация портала	Нет	Да	Да	Да	Нет	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
VPN и SD-WAN									
WEB-portal VPN	4.19	Типы приложений для публикации	Нет	Все Web-Based, FileShare, RDP in HTML, Citrix, IMAP in HTML	HTTP, HTTPS, FTP, SSH, RDP	HTTP, HTTPS, FileShare, DNS, H.323, SMTP, POP3, Telnet, SSH, LotusNote, Terminal Service, VNC, MSSQL Server, Citrix ICA (old version), MSN, Sinfor DNet, NetMeeting base, NetMeeting desktop, FTP (port/pasv mode), Citrix ICA (latest version), ORACLE, MYSQL, Other (ICMP, UDP, TCP, any protocol)	Нет	Нет	Нет
	4.20	Публикация нескольких порталов (на разных IP-адресах)	Нет	Нет	Нет	Нет	Нет	Нет	Нет
	4.21	Распространение через портал Remote Access Client	Нет	Да	Нет	Да	Да	Нет	Нет
	4.22	Публикация собственных приложений на портале	Нет	Да	Нет	Да	Нет	Нет	Нет
	4.23	Авторизация пользователя по сертификату	Нет	Да	Да	Да	Нет	Нет	Нет
	4.24	Публикация портала на разных URL	Нет	Да	Да	Да	Нет	Нет	Нет
	4.25	Поддержка 2FA	Нет	Да	Да	Да	Нет	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
VPN и SD-WAN									
2FA	4.26	2FA + Remote Access VPN с клиентом	Реализовано через интеграцию с мультифактор.ру и Avanpost MFA+	Radius, TOTP, SMS, SMTP	Radius, TOTP, SMS	TOTP, Hardware ID	Radius (при интеграции с Multifactor), SMS, TOTP	Реализовано через интеграцию с мультифактор.ру в рамках отдельного продукта ViPNet Сервер многофакторной аутентификации	Нет
	4.27	2FA + Remote Access VPN с SSL-порталом	Нет	Radius, TOTP, SMS, SMTP	Radius, TOTP, SMS	TOTP, Hardware ID	Нет	Нет	Нет
Site-to-Site VPN	4.28	Поддерживаемые протоколы	Проприетарный протокол	IKEv1, IKEv2, IPSec	IKEv1, IKEv2	IKEv1, IKEv2, IPSec, проприетарный VPN	IKEv2, IPsec	IPlir	IKEv1, IKEv2, IPSec
	4.29	DPD / Tunnel Test	Нет	Да	Да	Да	Нет	Да	Да
	4.30	Инструменты диагностики VPN-соединений	Диагностика сети (ping, tracert, arp), просмотр соединений, командная строка (netstat, tcpdump и др.)	IkeView, SmartConsole	Нет	Логирование	Виджеты панели мониторинга, утилиты командной строки (ping, host, nslookup, tracepath, tcpdump, arping, ss (аналог netstat))	Группа команд iplir, диагностика сети (ping, tracert, arp), командная строка (netstat, tcpdump и др.)	Show VPN connections, show the in-kernel crypto policies, show all active IPsec Security Associations (SA), show the in-kernel crypto state, show status of IPsec process
	4.31	SA lifetime	Нет	Да	Да	Да	Да, с ограничениями	Нет	Да
	4.32	Аутентификация	Да	Да	Да	Да	Да	Да	Да
	4.33	Исключение из VPN-трафика на основании сервиса	Да	Да	Да	Да	Нет	Да	Да
	4.34	Алгоритмы шифрования	ГОСТ	DES, 3DES, AES-128, AES-256	DES; 3DES; AES128, AES192, AES256	DES, 3DES, AES/AES128, AES192, AES256, SM4, проприетарный_DES	AES256-GCM, AES256	ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018	aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, aes128ccm64, aes192ccm64, aes256ccm64, aes128ccm96,

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
									aes192ccm96, aes256ccm96, aes128ccm128, aes192ccm128, aes256ccm128, aes128gcm64, aes192gcm64, aes256gcm64, aes128gcm96, aes192gcm96, aes256gcm96, aes128gcm128, aes192gcm128, aes256gcm128, aes128gmac, aes192gmac, aes256gmac, 3des, blowfish128, blowfish192, blowfish256, camellia128, camellia192, camellia256, camellia128ctr, camellia192ctr, camellia256ctr, camellia128ccm64, camellia192ccm64, camellia256ccm64, camellia128ccm96, camellia192ccm96, camellia256ccm96, camellia128ccm128, camellia192ccm128, camellia256ccm128, serpent128, serpent192, serpent256, twofish128, twofish192, twofish256, cast128, chacha20poly1305

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
VPN и SD-WAN									
Site-to-Site VPN	4.35	NAT-T (NAT Traversal)	Да	Да	Да	Да	Да	Да	Да
	4.36	IKEv1 Aggressive Mode	Нет	Да	Да	Да	Нет	Нет	Да
	4.37	PFS (Perfect Forward Secrecy)	Нет	Да	Нет	Да	Да	Да, с ограничениями	Да
	4.38	NAT внутри VPN	Да	Да	Да	Да, с ограничениями	Да	Да	Да
	4.39	GRE over IPsec	Нет	Да	Да	Да	Нет	Да, с ограничениями	Да
	4.40	IPsec over GRE	Нет	Да	Да	Да	Нет	Да, с ограничениями	Да
	4.41	VPN со сторонними вендорами	Нет	Да	Да	Да	Да	Нет	Да
SD-WAN	4.42	SD-WAN	Нет	Да	Нет	Да	Нет	Нет	Нет
	4.43	Распределение пользователей (локальных и доменных) по каналам	Нет	Да	Нет	Нет	Нет	Нет	Нет
	4.44	Распределение трафика приложений/сайтов по каналам	Нет	Да	Нет	Да	Нет	Нет	Нет
	4.45	Мониторинг трафика	Нет	Да	Нет	Да	Нет	Нет	Нет
	4.46	IPsec over SD-WAN	Нет	Да	Нет	Да, с ограничениями	Нет	Нет	Нет
	4.47	Интеграция с модулями URL Filtering / Application Control	Нет	Да	Нет	Да, с ограничениями	Нет	Нет	Нет
	4.48	Типы фильтров в политиках SD-WAN	Нет	Все категории AppControl и URLFiltering	Нет	Все категории AppControl	Нет	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Отказоустойчивость и кластеризация									
Кластеризация	5.1	Требования к нодам кластера	Требуется одинаковое оборудование (модель, ОС, патчи)	Требуется одинаковое оборудование (модель, ОС)	Требуется одинаковая версия ОС	Требуется одинаковое оборудование (модель, ОС)	Обе ноды должны иметь одну версию системы, идентичную вплоть до номера сборки. Также интерфейсы на обеих нодах должны быть настроены идентично	Для ViPNet Coordinator HW: одинаковая платформа и версия ПО. Для ViPNet Coordinator VA: одинаковые параметры эмулируемого аппаратного обеспечения (количество процессоров, ОЗУ и сетевых интерфейсов)	Обе ноды должны иметь одну версию системы
	5.2	Механизмы резервирования кластера	Проприетарный протокол	VRRP и ClusterXL	VRRP	Кастомизированный VRRP	Проприетарный протокол	Проприетарный протокол	VRRP
	5.3	VIP-адрес и адреса физических интерфейсов должны принадлежать одной подсети	Да	Нет	Нет	Нет	Нет	Да	Да
	5.4	Дополнительная лицензия для кластера	Нет	Нет	Нет	Да	Нет	Нет	Нет
	5.5	Добавление сетевых интерфейсов после сборки кластера	Да	Да	Да	Да	Нет	Да	Да
	5.6	Поведение при отключении сетевого интерфейса	Переключение мастер-ноды	Зависит от настроек	Переключение мастер-ноды	Переключение мастер-ноды	Переключение мастер-ноды	Переключение мастер-ноды	Переключение мастер-ноды
	5.7	GARP	Да, с ограничениями	Да	Да	Да	Да	Нет	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Отказоустойчивость и кластеризация									
Кластеризация	5.8	Время переключения между нодами	Менее 1 секунды	Менее 1 секунды	Менее 1 секунды	Менее 3 секунд. Время переключения зависит от причины сбоя и значений параметра Heartbeat Interval и может быть от «без задержек» до 3x Heartbeat Interval	5-15 секунд	Менее 15 сек.	Не больше 3 секунд
	5.9	Потери пакетов при выходе из строя одного линка при использовании LoadSharing Active/Active	При параметрах по умолчанию: до 50 icmp пакетов; есть настройки, позволяющие изменить периодичность проверки работоспособности канала	До 2 пакетов	1-2 пакета	Не тестировалось	2-3 пакета	Нет	До 3 пакетов
	5.10	Синхронизация сессий	Да	Да	Да	Да	Нет	Да	Да
	5.11	Кластер системы централизованного управления	Да	Да	Да	Да	Нет	Нет	Нет
	5.12	Кластер системы централизованного логирования	Да	Да	Нет	Нет	Нет	Нет	Нет
	5.13	Просмотр состояния кластера	Да	Да	Да	Да	Да	Да	Да
	5.14	Тип кластера	Active-Passive	Active-Passive, Active-Active	Active-Passive, Active-Active	Active-Passive	Active/Standby	Active-Passive	Active-Passive
	5.15	VMAC	Нет	Да	Нет	Да	Нет	Да	Нет
	5.16	Количество нод кластера	2	VRRP – 2, ClusterXL – 5, Maestro – от 8	До 4	2	2	2	2 или более

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Централизованное управление и отчетность									
Централизованное управление	6.1	Выделенный сервер управления	Да	Да	Да	Да	Да	Да	Нет
	6.2	Импорт правил/политик с локального МСЭ	Нет	Да	Да	Не тестировалось	Нет	Нет	Нет
	6.3	Кластер сервера управления	Да	Да	Да	Да	Нет	Нет	Нет
	6.4	Установка на ВМ	Да	Да	Да	Да	Да	Да	Нет
			Продолжит работу	Продолжит работу	Продолжит работу	Продолжит работу. Если локальное управление не запрещено, то будет возможность редактировать все из консоли самого МСЭ	Продолжит работу	Продолжит работать	Нет
	6.5	Поведение МСЭ при отключении сервера управления	Да	Да	Да	Да	Да	Да	Нет
	6.6	Экспорт и резервное копирование политик	Да	Да	Да	Да	Нет	Да	Нет
Централизованное логирование	6.7	Выделенный сервер логирования	Да	Да	Да	Нет	Локальное логирование, отправка на сторонний сервер через Syslog	Локально, централизованно	Нет
	6.8	Режим логирования	Локально, централизованно	Локально, централизованно	Локально, централизованно	Локально, внешний log-сервер	Да	Да	Нет
	6.9	Автоматическая выгрузка логов на сторонний сервер	Да	Да	Да	Да	RAW формат в БД ClickHouse	RAW text log, SQLite	Нет
	6.10	Формат хранения логов	Логи хранятся в БД. Есть возможность выгрузки в виде файлов xml, csv	RAW text log, индексы в базе PostgreSQL	Логи хранятся в БД	Встроенная БД	Да	Да	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Централизованное управление и отчетность									
Централизованное логирование	6.11	Регистрация и управление зарегистрированным и инцидентами	Да, с ограничениями	Да	Да	Да	МЭ, IPS/IDS, Web Application Firewall, Контент-Фильтр, Контроль приложений	Все модули	Нет
Логирование и отчёты	6.12	Модули с логированием	Все модули	Все модули	Все модули	FW, IPS, Botnet, AppControl	Нет	Нет	bandwidth, cluster, conntrack-sync, content-inspection, dhcp, dns, firewall, https, lldp, log, nat, ndp, openvpn, protocol (routing protocols), snmp, traffic (traffic dumps), vpn, vrrp, webproxy
	6.13	Выгрузка логов	Да	Да	Да	Да	Да	Да	Да
	6.14	Отправка логов на сторонний сервер	Да	Да	Да	Да	Да	Да	Да
	6.15	Типы отчеты	Встроенные, пользовательские	Встроенные, пользовательские	Встроенные, пользовательские	Встроенные	Встроенные, пользовательские	Нет	Нет
	6.16	Автоматические отчеты (по расписанию)	Да	Да	Да	Да	Да	Нет	Нет
	6.17	Типы логирования (вся сессия, начало сессии, выбранное кол-во пакетов и т. д.)	В зависимости от компонента	Per Connection, Per session, Detailed log, Extended Log	Начало сессии либо все пакеты сессии с возможностью установки ограничений на количество логируемых пакетов в единицу времени	Session start, Session stop	Вся сессия	Регистрировать все IP-пакеты или только заблокированные IP-пакеты	Вся сессия
	6.18	Виджеты для мониторинга трафика	Да	Да	Да	Да	Да	Да	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Интеграция									
LDAP	7.1	Использование пользователей из LDAP для создания политик	Да	Да	Да	Да	Да	Да	Да
	7.2	Права УЗ для интеграции с LDAP	Чтение домена	Чтение домена, доступ к WMI	Администратор домена	Чтение домена	Права на чтение каталога	Чтение домена	Права на чтение домена
	7.3	Поддержка более одного домена	Да, с ограничениями	Да	Да	Да	Да	Нет	Да, с ограничениями
	7.4	Требования к ПО для LDAP-аутентификации	Дополнительные требования не предъявляются	Для крупных инсталляций (больше 10 тысяч пользователей) — Identity Collector	Дополнительные требования не предъявляются	Дополнительные требования отсутствуют	Дополнительные требования не предъявляются	Дополнительные требования не предъявляются	Дополнительные требования не предъявляются
	7.5	Просмотр импортированных пользователей	Да, с ограничениями	Да	Да	Да	Да	Да	Нет
	7.6	Kerberos	Да	Да	Да	Да	Да	Нет	Нет
	7.7	Proxy-аутентификация	Да	Да	Да	Нет	Да	Да	Да
	7.8	Прозрачная аутентификация	Да	Да	Да	Да	Да	Нет	Нет
	7.9	Версия ОС LDAP-сервера	Windows Server 2008 и старше	Windows Server 2008 и старше	Windows Server 2008 и старше	Windows Server 2008 и старше, Linux с поддержкой OpenLDAP	Windows Server 2008 R2, 2012, 2016, 2019, 2022; Samba DC версии 4.0 и старше	Windows Server 2016, Windows Server 2012 R2	Windows Server 2012, 2016, 2019
	7.10	Secure LDAP	Да	Да	Да	Нет	Да	Да	Да
Radius	7.11	Интеграция с Radius	Нет	Да	Да	Да	Нет	Да, с ограничениями	Да
	7.12	Протоколы аутентификации при интеграции с Radius	Нет	PAP, MS CHAP2	Chap	PAP, CHAP, MS CHAP, MS CHAP2, EAP_MD5	Нет	Нет	PAP
	7.13	Использование нескольких Radius-серверов	Нет	Да	Да	Да	Нет	Нет	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Интеграция									
Radius	7.14	Приоритизации Radius-серверов	Нет	Да	Нет	Нет	Нет	Нет	Нет
ICAP	7.15	ICAP Server	Нет	Да	Нет	Нет	Нет	Нет	Нет
	7.16	ICAP Client	Да	Да	Да	Нет	Да	Да	Нет
	7.17	Возможность поддержки ICAP без установки дополнительных модулей	Да	Да	Да	Нет	Да	Да	Нет
	7.18	Необходимость указывать VIP-адрес в качестве ICAP Server адреса на стороне клиентов при использовании VIP-адреса для кластера	Нет	Да	Нет	Нет	Да	Нет	Нет
Эксплуатационные возможности									
Возможности диагностики	8.1	Модули диагностики в GUI	Работа с журналом мониторинга и отчетами	SmartConsole, SmartView, SmartLog, IkeVIEW, DiagnosticVIEW, Health Check Point, CPM Doctor, Log Doctor	Журналы, отчеты, захват пакетов	Packet Tracing, Route Tracing, Logs	Журнал событий, отчетность по модулям, виджеты Панели мониторинга	Работа с журналами, ARP-Таблица	Нет
	8.2	Модули диагностики в CLI	Утилиты для диагностики системы и сети, встроенные команды ping, tracert, arp, запись дампа, выгрузка отчетов и журналов и т.д.	CPView, Tcpdump, FWMonitor, Kernel Debug, IKE Debug, дебаг всех процессов	Журналы, захват пакетов	Packet Tracing, TCPDump, Logs, Traceroute, ping	ping, host, nslookup, tracepath, tcpdump, arping, ss (аналог netstat) и др.	Утилиты для диагностики системы и сети, встроенные команды ping, tracert, arp, запись дампа, работа с журналами и т.д.	Утилиты для диагностики системы и сети, встроенные команды ping, tracert, arp, запись дампа, работа с журналами и т.д.
	8.3	Доступ к логам ОС	Да	Да	Да, с ограничениями	Да, с ограничениями	Да	Да	Да
	8.4	Активация дебага отдельных модулей безопасности	Да, с ограничениями	Да	Да, с ограничениями	Нет	Да	Да	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Эксплуатационные возможности									
Обновление версии ПО	8.5	Обновление кластера	Да	Да	Да	Да	Да	Да	Да
	8.6	Обновление кластера без простоя	Да	Да	Да	Да	Да	Да	Да
	8.7	Резервное копирование при автоматическом обновлении	Нет	Нет	Да	Да, с ограничениями	Да	Нет	Нет
	8.8	Возможность отката к предыдущей версии	Нет	Да	Да	Да	Да	Да, с ограничениями	Нет
	8.9	Доступ к дистрибутивам на сайте производителя	Да	Да	Да	Да	Да	Нет	Нет
	8.10	Офлайн-обновления	Да	Да	Да	Да	Нет	Да	Да
	8.11	Обновление с web-ресурсов производителя	Да, с ограничениями	Да	Да	Да	Да	Да	Нет
	8.12	Обновление через систему централизованного управления	Да	Да	Да	Не тестировалось	Да	Да	Нет
Обновление лицензии	8.13	Офлайн-установка лицензии (без доступа в интернет)	Да	Да	Да	Да	Да	Да	Нет
Наличие API или других инструментов для миграции правил	8.14	API	Да	Да	Да	Да	Да, с ограничениями	Нет	Нет
	8.15	Модули, доступные через API	Сетевые объекты, правил МЭ и NAT	Все (SmartMove)	Все	Все	Все	Нет	Нет
	8.16	Загрузка политик через web-интерфейс	Нет	Да	Нет	Да	Да	Нет	Нет
	8.17	Загрузка политик через CLI	Нет	Да	Да	Да	Да	Нет	Нет

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Эксплуатационные возможности									
Наличие API или других инструментов для миграции правил	8.18	Поддержка миграции с других продуктов	Да	Да	Да	Нет	Да	Да	Нет
	8.19	Требуется ли установка стороннего ПО для модернизации политик/скрипта	Да	Нет	Нет	Нет	Нет	Нет	Нет

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ

ГРУППА ФУНКЦИОНАЛА	№ П/П	КЕЙС	КОНТИНЕНТ 4.1.7	CHECKPOINT R81.20	USERGATE 7.1.0	РЕШЕНИЕ КИТАЙСКОГО ВЕНДОРА 8.0	IDECO NGFW V16	VIPNET COORDINATOR HW5 5.3	INFOWATCH ARMA СТЕНА (NGFW)
Нагрузочное тестирование	9.1	Платформа	IPC-R1000	7000 Plus	-	7000 series	EX	HW5000	0
	9.2	Результаты теста вендора (EMIX, Гбит/с)	4,9	9,5	нет данных	12,5	5	1	7,8
	9.3	Результаты теста "Инфосистемы Джет" (EMIX, Гбит/с)	2,5	8,5	нет данных	12,5	0,75	1,22	6,2
	9.4	Комментарии	Значения других параметров при тестировании EMIX Throughput: PPS 0,35Mpps, CPS 2,5k, CC 1,64k	Значения других параметров при тестировании EMIX Throughput: PPS 1Mpps, CPS 8,47k, CC 4,98k	Нагрузочное тестирование для UserGate будет проведено после выхода релиза версии 7.1 для получения достоверных данных. Функциональные тесты UserGate 7.1.0 проводились на Release Candidate	Значения других параметров при тестировании EMIX Throughput: PPS 1,7Mpps, CPS 12,1k, CC 26,5k	Значения других параметров при тестировании EMIX Throughput: PPS 0,09Mpps, CPS 0,85k, CC 0,55k Основное влияние на производительность оказывал модуль Контроль приложений. При отключении данного модуля были получены следующие результаты: EMIX Throughput 1,7Гбит/с, PPS 0,2Mpps, CPS 2k, CC 1,2k	Значения других параметров при тестировании EMIX Throughput: PPS 0,14Mpps, CPS 1,2k, CC 1,12k	Значения других параметров при тестировании EMIX Throughput: PPS 0,73Mpps, CPS 5,8k, CC 6k