















Сравнение универсальных шлюзов безопасности USG (NGFW)

Архитектура решений

Параметр сравнения										
Поддерживаемые варианты исполнения	Аппаратное, виртуальное, облачное	Аппаратное, виртуальное, облачное	Аппаратное, виртуальное, облачное	Аппаратное	Аппаратное, виртуальное, облачное	Аппаратное, виртуальное	Аппаратное, виртуальное, облачное	Аппаратное, виртуальное	Аппаратное, виртуальное	Аппаратное, виртуальное, облачное
Используемая операционная система	FreeBSD	Linux CentOS	Собственная ОС UGOS (специализированная сборка Linux)	Собственная ОС ContinentOS (специализированная сборка Linux)	Debian	FreeBSD	Сборка Linux	Сборка Linux	Сборка Linux	Сборка Linux

Параметр сравнения										
Снапшоты	Да	Нет	Да	Да	Нет	Нет	Нет	Нет	Нет	Нет

Создание виртуальных частных сетей VPN

Параметр сравнения										
IPsec VPN client	Да	Да	Да	Да	Нет	Да	Да	Да	Да	Да
ГОСТ SSL VPN	Да	Да	Да	Да	Нет данных	Нет	Да	Да	Да	Да
Протоколы VPN	L2TP, PPTP, OpenVPN, WireGuard, OpenConnect	L2TP, PPTP, Wireguard и SSTP	L2TP, PPTP	L2TP	TLS	PPTP, SSTP, OpenVPN и WireGuard	PPTP, L2TP, OpenVPN	L2TP, PPTP	L2TP, PPTP	L2TP, PPTP

Функции межсетевого экранирования

Параметр сравнения										
Управление полосой пропускания	Да	Да	Да	Да	Да, LACP	Да	Да	Да	Да	Да
Статическая трансляция сетевых адресов SNAT (Static Network Address Translation)	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да
Динамическая трансляция сетевых адресов DNAT (Dynamic Network Address Translation)	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да
GeoIP	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да

Поддержка сетевых сервисов

Параметр сравнения										
Статическая маршрутизация	Да, статическая маршрутизация IPv4 и IPv6	Да, статическая маршрутизация IPv4 и IPv6	Да	Да, статическая маршрутизация IPv4 и IPv6	Да	Да	Да	Да	Да	Да
Динамическая маршрутизация	Да (BGP, IS-IS, LDP, OSPF, RIP)	Да (OSPF, BGP)	Да (OSPF, BGP, RIP)	Да (OSPF, BGP)	Да (OSPF, BGP)	Да (OSPF, BGP, RIP)	Да (IGMP, OSPF, BGP, RIP)	Да, OSPF	Да	Да, PAT

Основные функции безопасности

Параметр сравнения	 TRAFFIC INSPECTOR NEXT GENERATION	 ideco	 UserGate	 КОД БЕЗОПАСНОСТИ	 pt	 ИНТЕРНЕТ КОНТРОЛЬ СЕРВЕР	 numa TECHNOLOGY	 SOLAR	 ViPNet Virtual Private Network	 Diamond VPN/FW
Аутентификация	Локальная база пользователей, LDAP, LDAPS, Radius, RADIUS, двухфакторная аутентификация, Captive Portal, NTLM в AD (SSO), Kerberos в AD (SSO), IP+MAC	Локальная база пользователей, LDAP в Microsoft AD, Kerberos в AD (SSO)	Active Directory, Kerberos, RADIUS, LDAP, Captive Portal, TACACS+, 2FA.	Локальная база пользователей, прозрачная аутентификации по протоколу Kerberos в AD (SSO), Captive Portal, локального агента аутентификации, Браузерная аутентификация SSO в AD	Интеграция с AD и OpenLDAP	Авторизация пользователей на AD, LDAP или через NTLM	PSK, Radius	IP-адресам, Kerberos (Negotiate), NTLM, NTLM + Negotiate, Basic, прозрачная аутентификация. Интеграция с AD	ViPNet TLS Gateway, ViPNet SafeBoot	Нет данных
Поддержка глубокого пакетного анализа (Deep Packet Inspection, DPI)	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да
Поддержка расшифрования входящего и исходящего трафика по протоколу SSL/TLS	Да	Да	Да	Да	Да	Да, в HTTP-прокси	Да	Да	Да	Да
Система обнаружения / предотвращения вторжений (IDS/IPS)	Да, IDS/IPS Suricata с методом захвата пакетов NETMAP	Да, IDS/IPS Suricata	Да, модуль IPS с собственными сигнатурами	Да, модуль IPS с собственными сигнатурами	Собственная	Да, IDS/IPS Suricata	Да	IPS	Да	Нет
Контроль приложений (Application Control)	Да, L7 (nDPI, libpcap, Packet Filter)	Да, nDPI	Да, модуль L7	Да	Да, nDPI	Да, реализация на основе библиотеки nDPI	Нет	DPI	Нет	Да

Основные функции безопасности

Параметр сравнения										
Контроль доступа (блокирование / разрешение, отслеживание)	Да (по протоколам HTTP, FTP, DNS, DHCP, SMTP)	Да, HTTP, HTTPS	Да, определение приложений в транзитном трафике, блокирование известных приложений, блокирование всех неизвестных приложений	Да, распознается более 2600 приложений VoIP, социальных сетей, файлообмена, видеотрансляций, корпоративных инфокоммуникационных систем	Да	Да (все протоколы, распознаваемые nDPI)	Нет	Да	Да	Нет
Антивирусная защита (Antivirus)	Да (ClamAV, Kaspersky Antivirus)	Да, Kaspersky Antivirus	Да, собственный и Kaspersky	Защита от вирусов осуществляется путем запрета доступа к URL-адресам с низкой репутацией (Malicious URL block)	Да	Да (ClamAV, Kaspersky Antivirus)	Да	Да	Нет	Нет
Защита почтового трафика (безопасность почты, антиспам)	Да, использование rspamd, ClamAV	Да (модуль Kaspersky Anti-Spam)	Да, модуль защиты почтового трафика	Нет	Нет	Да (общедоступные базы для SpamAssassin и rspamd, проприетарные базы Kaspersky Anti-Spam)	Да	Нет	Да	Нет
Веб-фильтрация	Да, контент-фильтр	Да, контент-фильтр	Да, модуль контентной фильтрации	Только запрет доступа к опасным ресурсам на основе данных Kaspersky Feed	Да	Да (SkyDNS, Kaspersky Web Filter)	Да	Да, модуль Solar webCat	Да	Да
Поддержка создания черных и белых списков URL-адресов	Да, с возможностью подгружать готовые списки внешних источников	Да	Да	Да	Да	Да	Да	Да	Да	Да
Поддержка возможности блокировки по произвольному списку URL и IP	Да, том числе по DNS	Да	Да	Да	Да	Да	Да	Фильтрация трафика по URL-адресам и категориям веб-ресурсов	Нет данных	Нет данных

Управление и кластеры

Параметр сравнения										
Поддерживаемые режимы кластеризации	Аварийное переключение, синхронизация состояний (вручную, либо за какой-то промежуток времени)	Аварийное переключение, синхронизация состояний	Active/Passive, Active/Active	Active/Passive	Active/Passive	Нет	Active/Passive	Active/Passive	кластер высокой доступности	Active/Passive
Поддерживаемые режимы переключения при сбоях	Переключение на резервное оборудование или резервный канал	Переключение на резервное оборудование или резервный канал	Переключение на резервное оборудование или резервный канал	Переключение на резервное оборудование или резервный канал	Переключение на резервное оборудование или резервный канал	Нет	Переключение на резервное оборудование или резервный канал	Переключение на резервное оборудование или резервный канал, active/active	Переключение на резервное оборудование или резервный канал, active/active	Переключение на резервное оборудование или резервный канал, active/active
Максимальное поддерживаемое количество устройств в кластере	2 в режиме Active-Passive, без ограничений в конфигурации Кластер	2 в режиме Active-Passive, без ограничений в конфигурации Кластер	2 в режиме Active-Passive, без ограничений в конфигурации Кластер	2	2 в режиме Active-Passive	Нет	Нет данных	До 64	Нет данных	Нет данных
Централизованное управление	Мастер-узел - Подчиненный узел (Central Management System)	Ideco CENTER (отдельный продукт)	«UserGate Management Center (вспомогательный компонент)»	Нет	Нет	Нет	Нет	Да	Нет	ЦУМ (центр управления и мониторинга)

Мониторинг работы и система отчётности

Параметр сравнения										
Графическое представление показателей мониторинга	Анализ при помощи RRDTool, NetFlow. Производительность системы, уровень загрузки ресурсов ЦП, памяти, дискового пространства. Входящий/исходящий трафик в реальном времени и за интервал, использование портов, DNS-трафик, статистика по сетевым подключениям, пропускная способность сети и задержки. Данные о пользователях: время на сайте, страницы просмотра.	Анализ загрузки процессора, оперативной памяти и интерфейсов сервера, а также активность пользователей.	Объем потребленного трафика пользователями (приложениями и т.п), авторизации пользователей с помощью Captive-портала, DNS-трафик.	Нет	Объем потребленного трафика пользователями (приложениями и т.п), DNS-трафик.	Объем потребленного трафика, DNS-трафик, лента поиска, подключение пользователей, информацию по сетям.	Производительность системы, уровень загрузки ресурсов ЦП, памяти, дискового пространства, пропускная способность сети и задержки, количество переданных и полученных пакетов, статистика по сетевым подключениям. Данные о пользователях: время на сайте, страницы просмотра.	Solar Dozor	Производительность системы, общий трафик, информация о пользователях и устройствах, статистика по событиям безопасности.	Общий трафик, производительность системы, статистика безопасности, пользователи и устройства.
Использование внешних систем отчётности	Да (syslog, wazuh-agent, SIEM по ICAP)	Да, SIEM	Да, на сервера SSH, FTP и Syslog	Нет	MaxPatrol SIEM	SIEM	SIEM	Syslog	SIEM	Syslog, SIEM, SecuReporter

Сертификация

Параметр сравнения										
Сертификаты	Сертификат ФСТЭК № 4692 от 13.07.2023, действует до 13.07.2028	Сертификат ФСТЭК № 4503 от 28.12.2021, действует до 28.12.2026	Сертификат ФСТЭК № 3905 от 26.03.2018, действует до 26.03.2026	Сертификат ФСТЭК № 4496 от 14.12.2021, действует до 14.12.2026	Сертификат ФСТЭК № 4877 от 19.11.2024, действует до 19.11.2029	Сертификат ФСТЭК № 4832 от 02.08.2024, действует до 02.08.2029	Сертификат ФСТЭК № 4199 от 26.12.2019, действует до 26.12.2024 (окончание срока технической поддержки - 31.12.2034)	Сертификат ФСТЭК № 4784 от 05.03.2024, действует до 05.03.2029	Сертификат ФСТЭК № 4501 от 28.12.2021, действует до 28.12.2026	Сертификат ФСТЭК № 4066 от 24.01.2019, действует до 24.01.2029