

Как совместить функции NGFW и ГОСТ VPN в одном устройстве

Виталий Беличко

infotecs



ViPNet Coordinator HW 5.3



История версий



Сертификация

ФСБ России

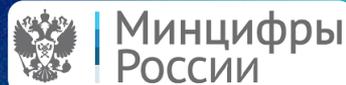
- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

- Межсетевой экран тип «А» и тип «Б» 4 класса
- COB уровня сети 4 класса
- 4-й уровень доверия средств защиты информации

Минцифры России и Минпромторг России

- В реестре российского ПО/ПАК и реестре РЭП

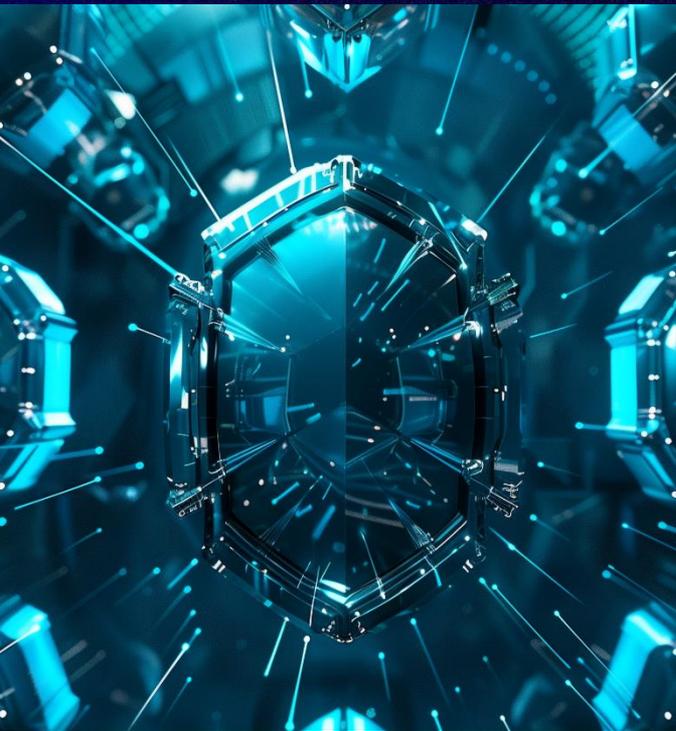


Межсетевое экранирование



- Межсетевой экран с контролем состояния сессий
- Выявление и блокировка более 2000 прикладных протоколов и приложений (DPI) **NEW**
- Выявление приложений, трафик которых шифруется или маскируется **NEW**
- Фильтрация трафика для заданного пользователя (AD, LDAP) **NEW**

Предотвращение вторжений **NEW**



- Работа как в режиме предотвращения вторжений (IPS), так и обнаружения (IDS) с фиксацией событий
- Сигнатурный и эвристический методы анализа трафика
- Автоматизированное обновление баз правил с сервера обновлений
- База правил регулярно обновляется специалистами ГК ИнфоТеКС для поддержания в актуальном состоянии

VPN с ГОСТ шифрованием



- VPN-шлюз сетевого и канального уровня
- Remote Access VPN (ViPNet Client)
- ГОСТ 34.12-2018, ГОСТ 34.13-2018 («Кузнечик» и «Магма») **NEW**
- ГОСТ 28147-89 для обратной совместимости
- IPsec 6 – протокол безопасности сетевого уровня **NEW**

Служебная криптография

1

**Защита канала
управления**
IPLir, TLS

2

**Аутентификация
администраторов**
Сертификаты на токене

3

**Защита резервных
копий конфигурации**
VBE, ECF

4

**Контроль
целостности**
Система, Журналы

5

**Проверка
обновлений**
ПО, БРП
конфигурации

Сетевые функции

- HA cluster с синхронизацией таблицы открытых соединений
- Расширенная статическая маршрутизация (Policy based routing)
- Динамическая маршрутизации (OSPF, BGP **NEW**)
- Поддержка VLAN
- Агрегирование сетевых интерфейсов (802.3ad, LACP)
- Поддержка Jumbo-кадров и Path MTU Discovery
- Приоритизация трафика (QoS, ToS, DiffServ)
- Встроенный DHCP-, DNS-, NTP-сервер
- SNMP, Syslog, Syslog (CEF), SSH, HTTPS

Аппаратные платформы

HW50



HW1000



HW2000



HW100



HW5000



Малые офисы и филиалы

Предприятия среднего
бизнеса

Крупные предприятия,
ЦОД

VIPNet Coordinator VA 5

Поддерживаемые гипервизоры:

- KVM, QEMU-KVM и Proxmox VE
- Астра Брест ^{DEV}, zVirt ^{DEV}, SharxBase
- VMware ESXi
- VMware Workstation
- Microsoft Hyper-V Server
- Oracle VM Server
- Oracle VM VirtualBox



Ролевая модель доступа



Тип записей

Независимые локальные УЗ
Централизованные из Prime



Роли

Администратор
Пользователь (Аудитор)



Способы аутентификации

Пароль
Сертификат



Поддержка USB токенов

- Рутокен ЭЦП 2.0
- Рутокен ЭЦП 3.0
- JaCarta-2 ГОСТ

VIPNet Prime

- Программный комплекс под Linux
- Управление с помощью веб-консоли
- Единая предметная область
- Управление лицензиями
- Интеграция с MS AD
- Многопользовательский доступ
- Ролевая модель SSO

Многофункциональный МЭ

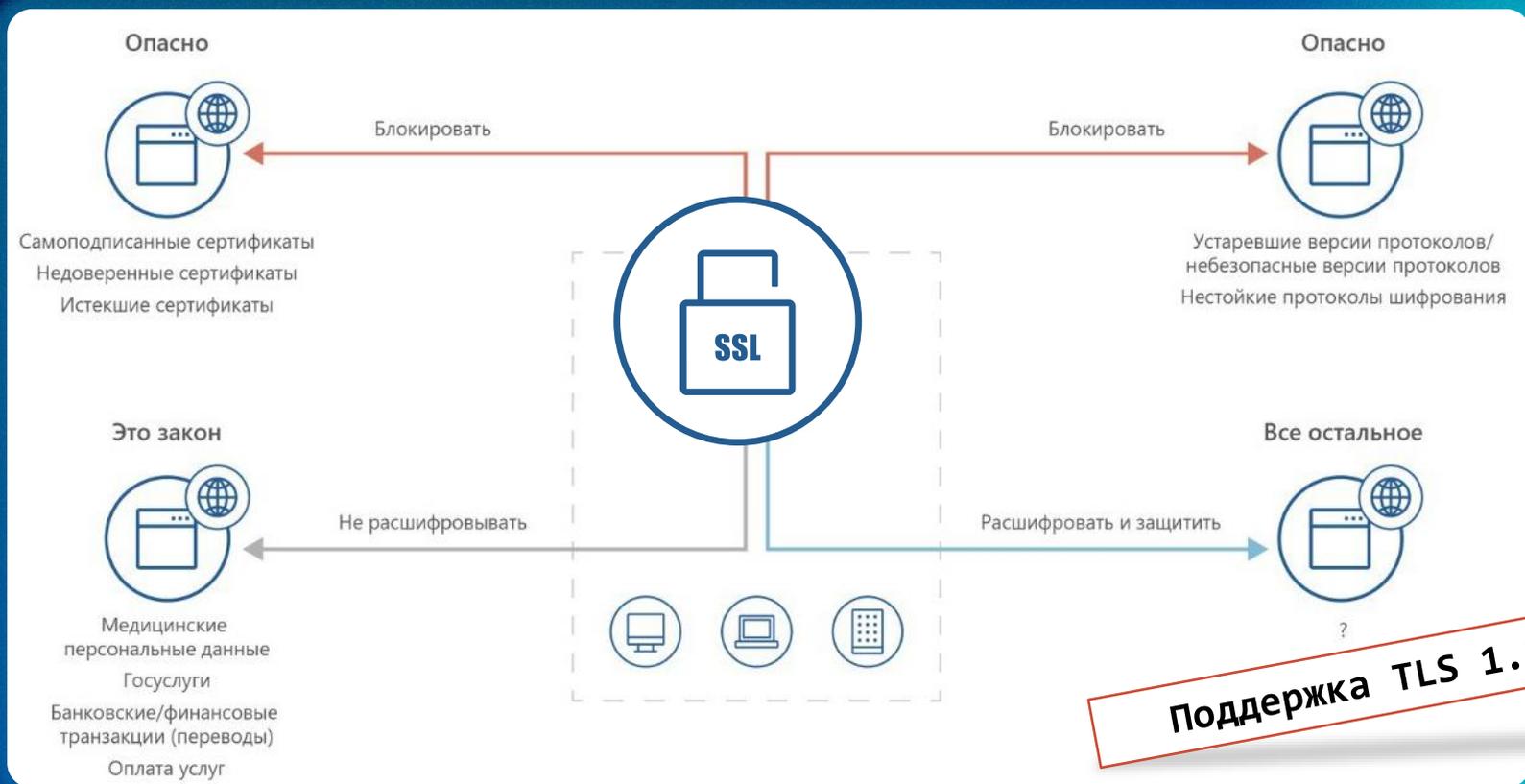


VIPNet Coordinator HW 5.4

- SSL/TLS-инспекция
- URL-фильтрация
- Блокировка по GEO-IP
- Обнаружение вредоносного ПО
- Расширение возможностей ICAP
- Журнал сетевых сессий
- Локальные учетные записи + новая роль
- Поддержка протокола BFD
- Расширение кол-ва интерфейсов
- Поддержка HW50 A1



SSL/TLS-инспекция



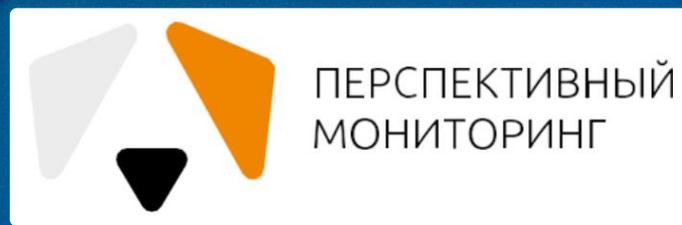
Поддержка TLS 1.3

URL-фильтрация

100M веб-ресурсов

80 категорий

+15% ежемесячный
прирост базы



Блокировка по GEO-IP

The screenshot shows the ViPNet Coordinator HW web interface. The main content area is titled "Группы объектов" (Object Groups) and has a sub-tab "Страны" (Countries) selected. A search bar and a "Обновить из файла" (Refresh from file) button are visible. A table lists countries with their flags and codes. The "Антигуа и Барбуда" (Antigua and Barbuda) entry is highlighted. A right-hand panel shows details for "Антигуа и Барбуда", including a message "Объект не используется" (Object not used) with a blue arrow pointing to the right, and a section for "Общая информация" (General information) showing the country name and code "AG".

ViPNet Coordinator HW | Admin 99+

Группы объектов

Узлы ViPNet IP-адреса Интерфейсы Протоколы Расписания Страны

Поиск Обновить из файла Последнее

Страна	Код
Афганистан	AF
Албания	AL
Алжир	DZ
Американское Самоа	AS
Андорра	AD
Ангола	AO
Ангилья	AI
Антарктида	AQ
Антигуа и Барбуда	AG
Аргентина	AR
Армения	AM
Аруба	AW

Антигуа и Барбуда

Список применений группового объекта

Объект не используется

Общая информация

Страна: Антигуа и Барбуда

Код: AG

Список подсетей

Обнаружение вредоносного ПО

The screenshot displays the 'ViPNet Coordinator HW' interface. The top navigation bar includes a search icon, a refresh icon, and user information for 'Admin' with 99+ notifications. The left sidebar contains a menu with items such as 'Состояние системы', 'Журналы', 'Статистика', 'Межсетевой экран', 'Защищённая сеть (VPN)', 'Предотвращение вторжений', 'Прикладные службы', 'Сетевые настройки', 'Маршрутизация', and 'Системные настройки'. The main content area is titled 'Предотвращение вторжений включено' and is divided into two sections: 'База правил IPS' and 'Обнаружение вредоносного ПО'. Each section includes a 'Обновить базу' button and a link to 'Настройки обновления с сервера'. The 'База правил IPS' section shows a release date of 27 May 2021, 15:00, an update server of updateids.infotecs.ru, and an expiration date of 13 May 2022, 03:00. The 'Обнаружение вредоносного ПО' section shows a release date of 27 May 2021, 15:00, an update server of updatemd.infotecs.ru, and an expiration date of 13 May 2022, 03:00.

ViPNet Coordinator HW | Admin | 99+ | Info

Предотвращение вторжений включено 🔒

Правила IPS | Методы анализа

База правил IPS Обновить базу | Настройки обновления с сервера

Дата выпуска базы: от 27 мая 2021, 15:00 | Сервер обновления: updateids.infotecs.ru
Действует до: 13 мая 2022, 03:00 | Автоматическое обновление базы: Ежедневно в 23:59

Обнаружение вредоносного ПО Обновить базу | Настройки обновления с сервера

Дата выпуска базы: от 27 мая 2021, 15:00 | Сервер обновления: updatemd.infotecs.ru
Действует до: 13 мая 2022, 03:00 | Автоматическое обновление базы: Ежедневно в 23:59

Расширение возможностей ICAP

The screenshot shows the 'ViPNet Coordinator HW' interface. The top navigation bar includes a search icon, a refresh icon, and a user profile 'Admin' with a notification bell showing '99+'. The left sidebar contains a menu with items like 'Состояние системы', 'Журналы', 'Статистика', 'Мехсетевой экран', 'Защищённая сеть (VPN)', etc. The main content area is titled 'ICAP-серверы' and features a search bar and a '+ Добавить ICAP-сервер' button. Below is a table of configured servers.

Статус	Имя сервера	Режим и тип	Адрес и порт	Путь к ICAP-серверу	Передаваемые параметры
🟢	Dr.Web-ICAP Удалённый антивирус Dr.Web	Инспекция трафика Антивирус (av)	● 192.168.15.22:1344	Входящего: /incoming-traffic Исходящего: /outgoing-traffic	Имя пользователя с заголовком: X-Aut IP-адрес с заголовком: X-Client-Ip MAC-адрес с заголовком: X-Client-Mac
🟢	ATHENA Песочница ATHENA	Инспекция трафика Песочница (sandbox)	● 192.168.15.92:1344	Входящего: /incoming-traffic	IP-адрес с заголовком: X-Client-Ip MAC-адрес с заголовком: X-Client-Mac
🟢	Solar Dozor DLP-система Solar	Инспекция трафика Система предотвращения у	● 192.168.1.15:1344	Исходящего: /outgoing-traffic	Выкл.
🟡	ICAP-сервер	Зеркалирование трафика	● 192.168.15.22:1344	Входящего: /incoming-traffic	Выкл.

Below the table, a red-bordered box highlights the inspection capabilities for the selected server:

- Инспекция: SSL/TLS-инспекция
- Антивирус (av)
- Предотвращение вторжений (IPS)
- Песочница (sandbox)
- Обнаружение вредоносного ПО
- Предотвращение утечки данных (dlp)

Журнал сетевых сессий

Navigation icons: three circles, left arrow, right arrow, search, refresh, plus, share.

Журнал сессий

Поиск Результат фильтрации за последний час, с 20.06.2024 13:39:41

Дата и время	Завершение	Состояние	Источник	Назначение	Пользователь сети	Протокол
2020.06.11 16:45:31	17:55:31	● Завершена	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP
2020.06.11 16:45:31	2020.06.12 13:23:54	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP

- Состояние системы
- Журналы
 - Журнал аудита
 - Журнал IP-пакетов
 - Журнал сессий
 - Журнал СКЗИ
 - Журнал MFTP
 - Журнал DNS-запросов
 - Системный журнал
- Статистика
- Межсетевой экран
- Защищённая сеть (VPN)
- Предотвращение вторжений
- Прикладные службы
- Сетевые настройки

Локальные учетные записи

- новая роль «Сетевой администратор»

The screenshot displays the 'Учётные записи' (Accounts) section of the ViPNet Coordinator HW interface. The left sidebar contains navigation options: 'Статистика и журналы', 'Межсетевой экран', 'Прикладные службы', 'Сетевые настройки', 'Системные настройки', 'Общие', 'Сертификаты', 'Сервисные функции', 'Учётные записи', and 'Управляющие соединения'. The main content area shows 'Локальные учётные записи' (Local accounts) with a search bar, a filter icon, and a '+ Добавить' (Add) button. Below is a table of local accounts.

Имя учетной записи	Роль	Полное имя	Описание
● Superadmin (Вы)	Суперадминистратор		Встроенная учётная запись
● Admin	Администратор		
● Ivanov.Sergej	Администратор	Иванов Сергей Егорович	Инженер по технической ...
● Kononov.Roman	Администратор	Коновалов Роман Тимофеевич	Инженер по технической ...
● Pavlov.Mikhail	Администратор	Павлов Михаил Николаевич	Инженер по технической ...
● Auditor	Аудитор		
● Smirnov.Nikita	Аудитор	Смирнов Никита Михайлович	Инженер по технической ...
● User	Аудитор		

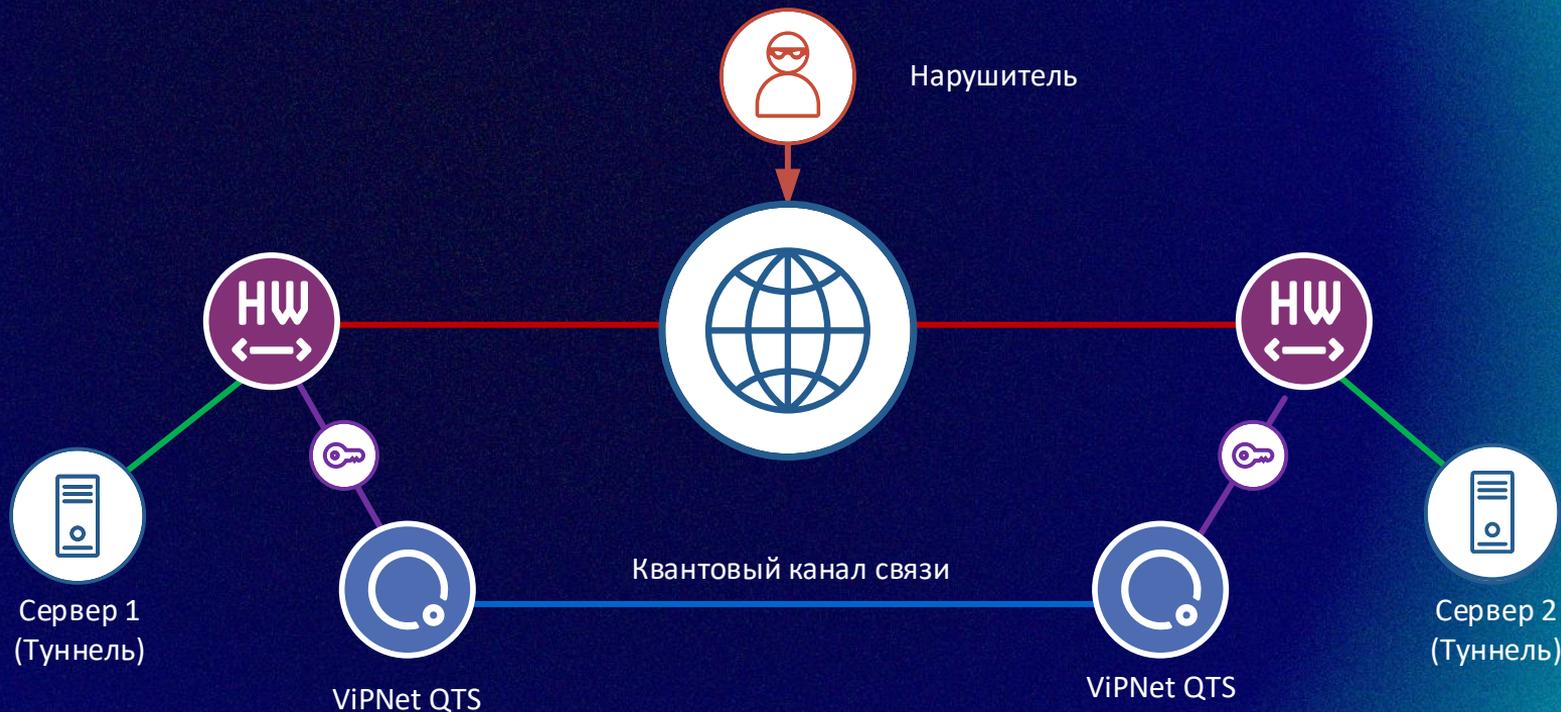
VIPNet Coordinator HW 5.5

Проект

- Поддержка HW10
- Интеграция с IDS MC:
 - Централизованное управление БРП
 - Поддержка профилей
 - Конструктор правил
- Расширение интеграции с AD:
 - Поддержка групп AD
 - Поддержка нескольких DC
- Поддержка RADIUS аутентификации
- Поддержка квантового распределения ключей (КРК)



Интеграция с КРК



Живой стенд на ТехноФесте 2025



Подписывайтесь
на наши соцсети,
там много интересного




infotecs

Спасибо за внимание!