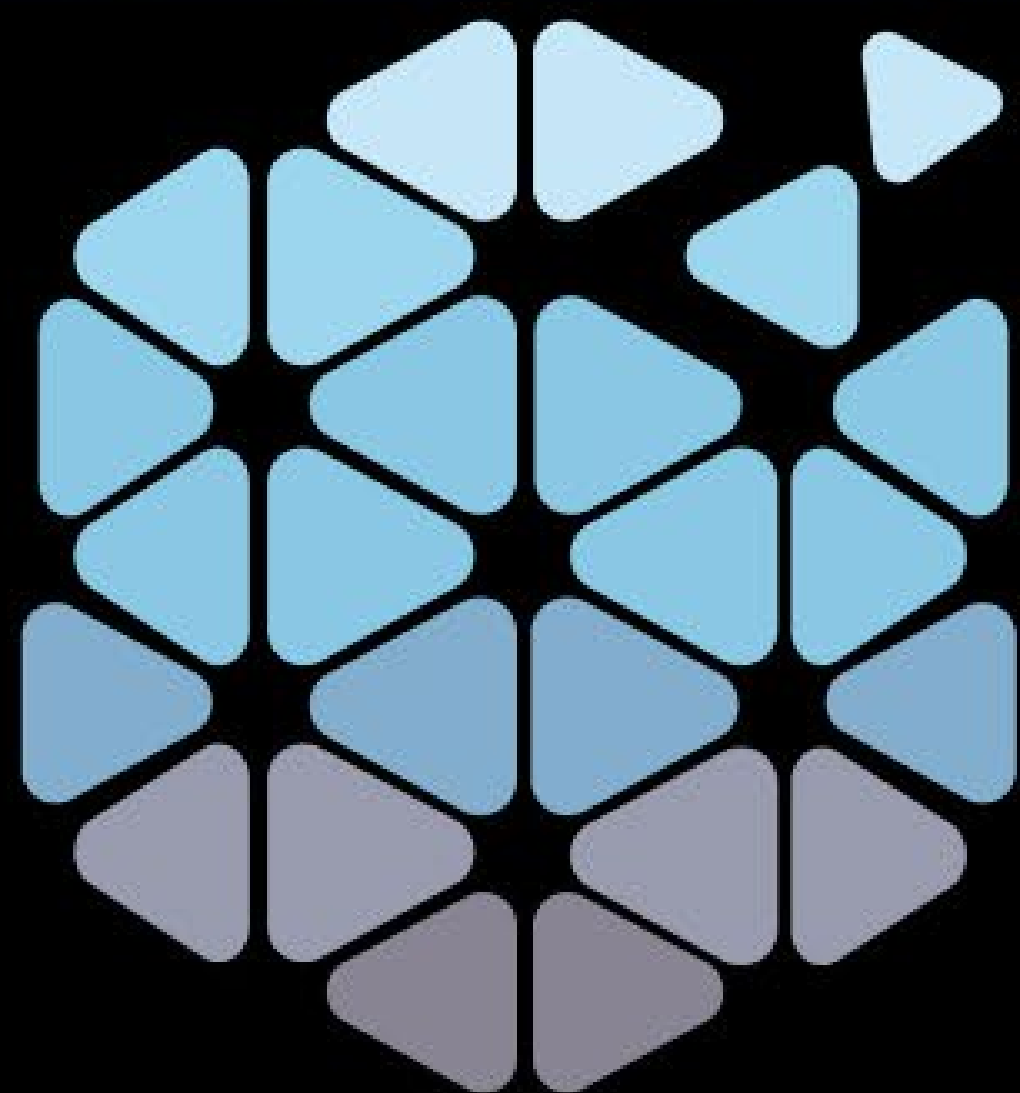




Сетевая Безопасность

[NGFW, WAF, NDR, VPN, ZTNA, Anti-DDOS, NAC, MFA]

09.12.2024

г. Москва, отель «Холидей Инн Сокольники»



Сетевая Безопасность



**Как совместить функции
NGFW и ГОСТ VPN
в одном устройстве**

Виталий Беличко

ИнфоТеКС, руководитель продуктового
направления


infotecs



Сетевая
Безопасность

Шлюзы безопасности ViPNet

ГОСТ VPN + FW (SPI)

Coordinator
Windows / Linux

Coordinator HW 4

IDS / IPS

IDS NS

AppControl (DPI)

xFirewall 4

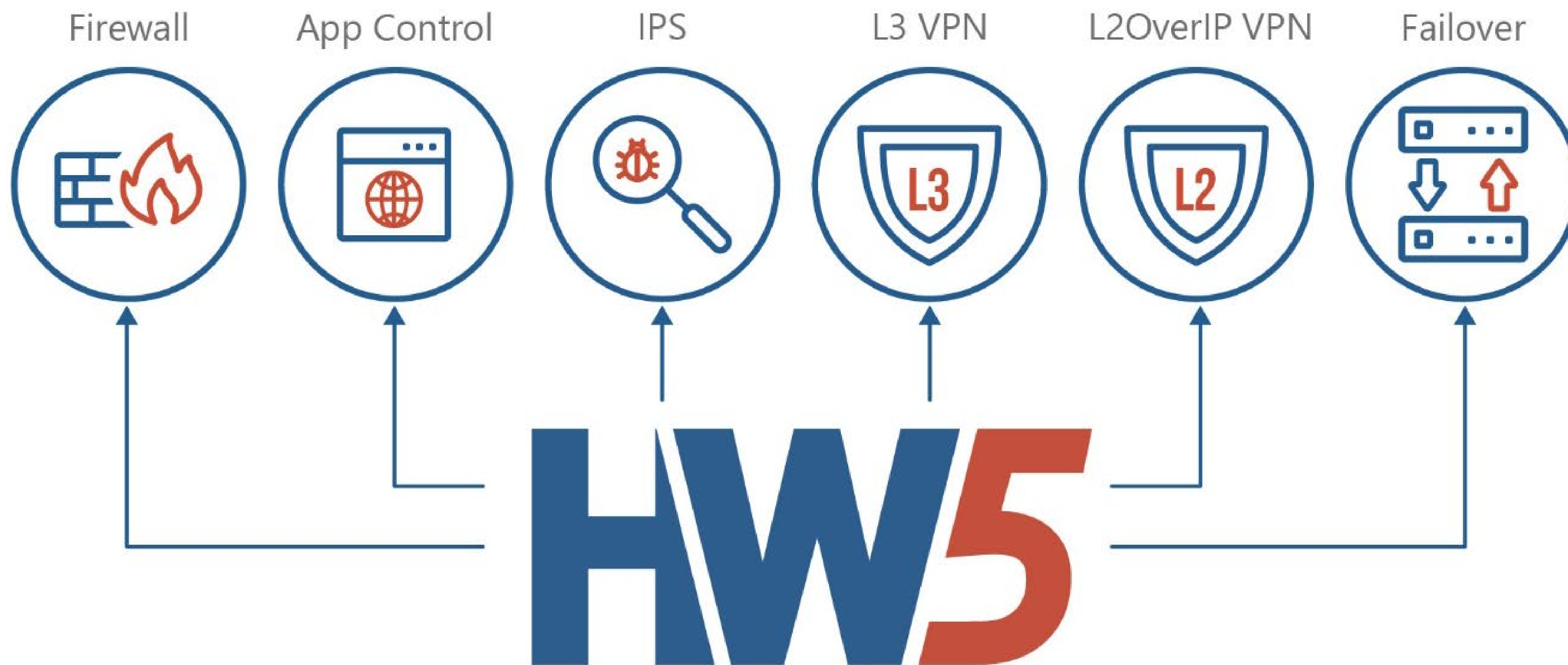
xFirewall 5

ViPNet Coordinator HW 5

ViPNet Coordinator HW 5



Сетевая
Безопасность

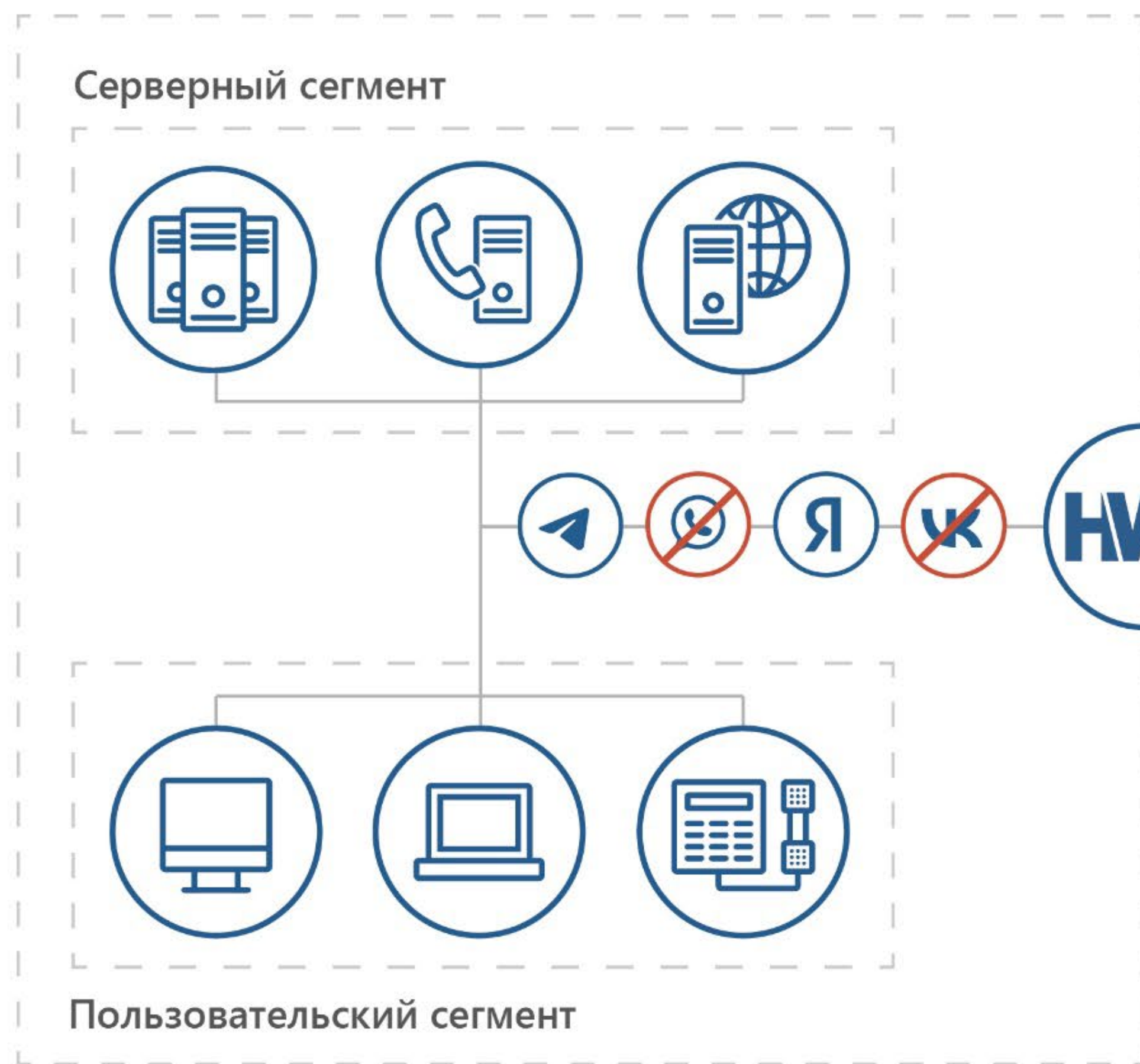




Сетевая
Безопасность

Типовая схема применения HW 5

Центральный офис



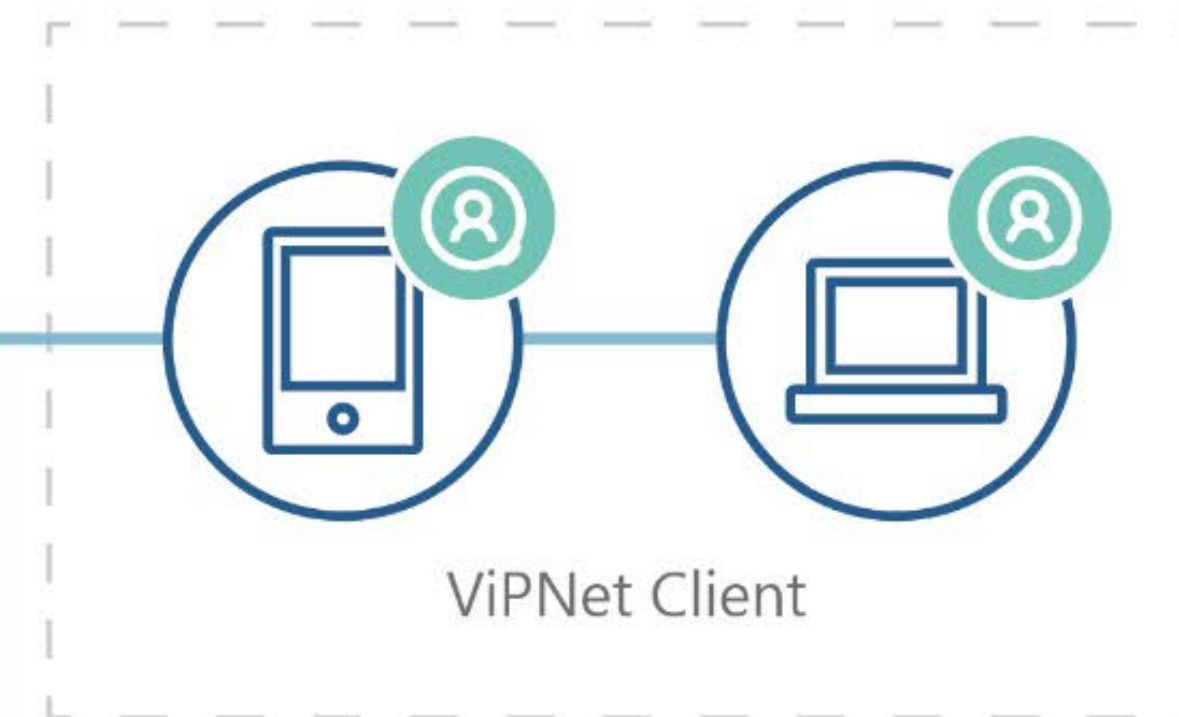
Злоумышленник



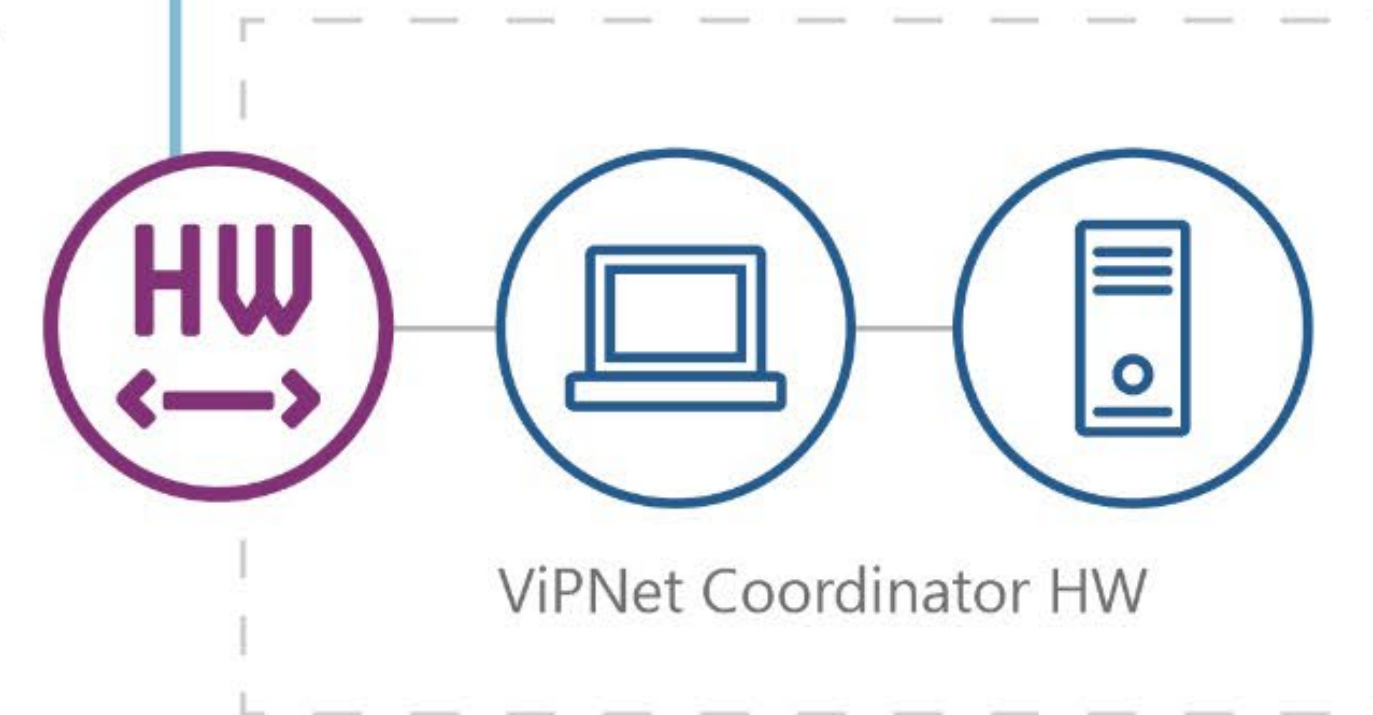
Интернет



Удаленные пользователи



Удаленный офис



Зашифрованный трафик

Открытый трафик

Сертификат ФСТЭК России (МЭ и СОВ)



Сетевая
Безопасность



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4831

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 июля 2024 г.

Выдан: 25 июля 2024 г.
Действителен до: 25 июля 2029 г.

Настоящий сертификат удостоверяет, что **ViPNet Coordinator HW 5**, разработанный и производимый АО «ИнфоТеКС», является межсетевым экраном и средством обнаружения (предотвращения) вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012), при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.465614.003ФО.

Сертификат выдан на основании технического заключения от 27.02.2024, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 01.07.2024, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В.Лютиков

Применение сертификатов на продукцию, указанной в настоящем сертификате соответствия, на объектах (объектах инфраструктуры) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4831

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 июля 2024 г.

Выдан: 25 июля 2024 г.
Действителен до: 25 июля 2029 г.

Настоящий сертификат удостоверяет, что **ViPNet Coordinator HW 5**, разработанный и производимый АО «ИнфоТеКС», является межсетевым экраном и средством обнаружения (предотвращения) вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012), при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.465614.003ФО.

Сертификат ФСБ России (СКЗИ КСЗ)



Сетевая
Безопасность



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4972 от "30" августа 2024 г.

Действителен до "30" августа 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы»

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet Coordinator HW 5 (исполнения: ViPNet Coordinator HW50 на аппаратных платформах: HW50 N1, HW50 N2, HW50 N3, HW50 N4; ViPNet Coordinator HW100 на аппаратных платформах: HW100 N1, HW100 N2, HW100 N3; ViPNet Coordinator HW1000 на аппаратных платформах: HW1000 Q4, HW1000 Q7; ViPNet Coordinator HW1000 C на аппаратных платформах: HW1000 Q5, HW1000 Q8; ViPNet Coordinator HW1000 D на аппаратных платформах: HW1000 Q6, HW1000 Q9; ViPNet Coordinator HW2000 на аппаратных платформах: HW2000 Q4, HW2000 Q5; ViPNet Coordinator HW5000 на аппаратных платформах: HW5000 Q1, HW5000 Q2) в комплектации согласно формуляру ФРКЕ.465614.003ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КСЗ и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 1056А-000501, 1056Б-000501, 1056В-000501, 1056В1-000501, 1056В2-000501, 1056Г-000501, 1056Д-000501.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.003ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.003ФО.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России


О.В. Скрибин

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4972 от "30" августа 2024 г.

Действителен до "30" августа 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet Coordinator HW 5 (исполнения: ViPNet Coordinator HW50 на аппаратных платформах: HW50 N1, HW50 N2, HW50 N3, HW50 N4; ViPNet Coordinator HW100 на аппаратных платформах: HW100 N1, HW100 N2, HW100 N3; ViPNet Coordinator HW1000 на аппаратных платформах: HW1000 Q4, HW1000 Q7; ViPNet Coordinator HW1000 C на аппаратных платформах: HW1000 Q5, HW1000 Q8; ViPNet Coordinator HW1000 D на аппаратных платформах: HW1000 Q6, HW1000 Q9; ViPNet Coordinator HW2000 на аппаратных платформах: HW2000 Q4, HW2000 Q5; ViPNet Coordinator HW5000 на аппаратных платформах: HW5000 Q1, HW5000 Q2) в комплектации согласно формуляру ФРКЕ.465614.003ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КСЗ и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

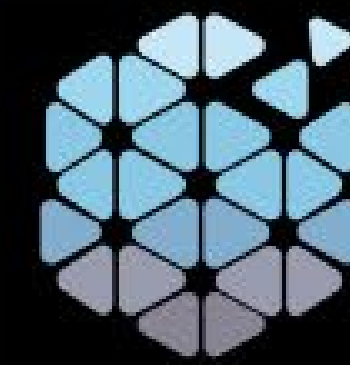
Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 1056А-000501, 1056Б-000501, 1056В-000501, 1056В1-000501, 1056В2-000501, 1056Г-000501, 1056Д-000501.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.003ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.003ФО.



Требования по сертификации



Сетевая
Безопасность

ФСБ России

- ✓ СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

- ✓ Межсетевой экран тип «А» и тип «Б» 4 класса
- ✓ СОВ уровня сети 4 класса
- ✓ 4-й уровень доверия средств защиты информации
- Многофункциональный межсетевой экран уровня сети **NEW**

Минцифры России и Минпромторг России

- ✓ В реестре российского ПО, ПАК и РЭП



Минцифры
России



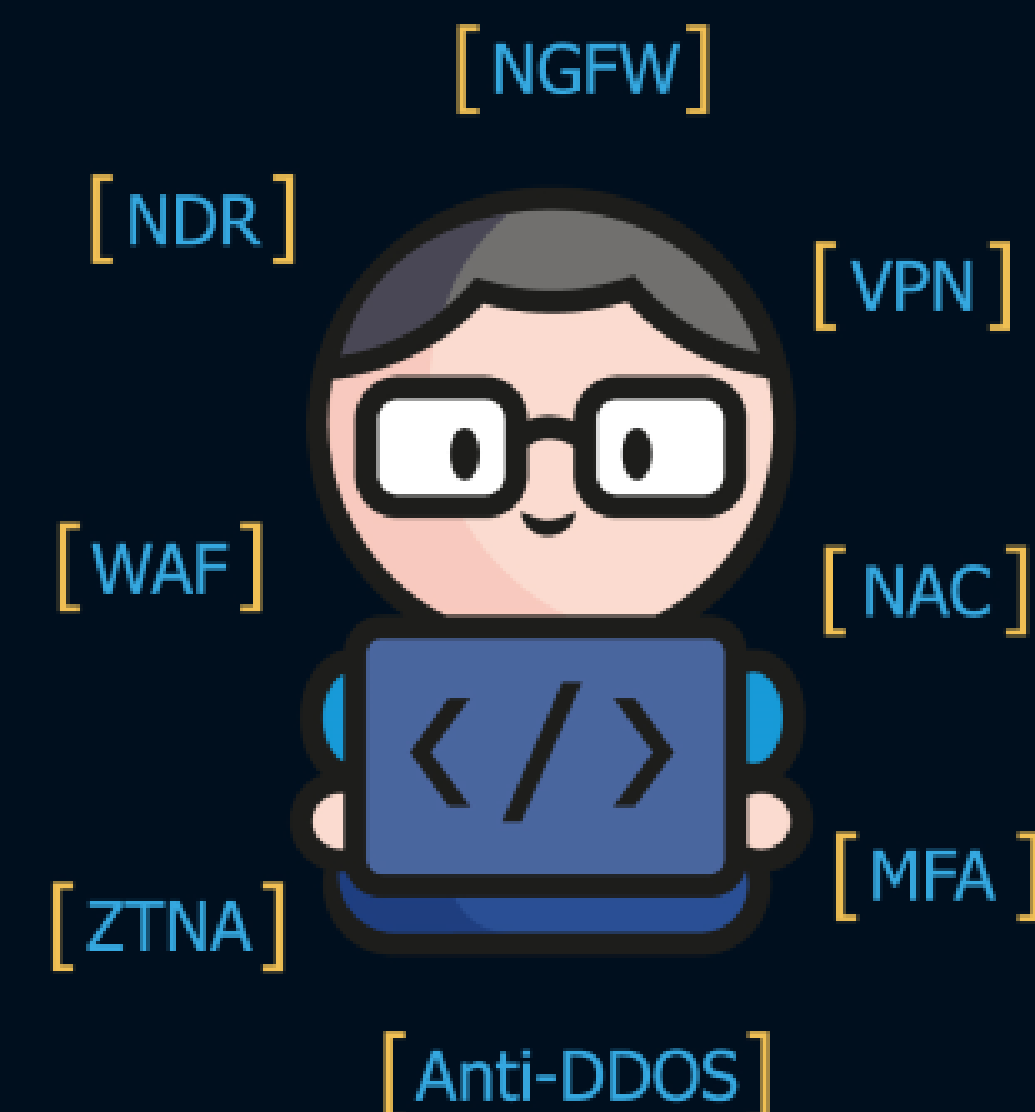
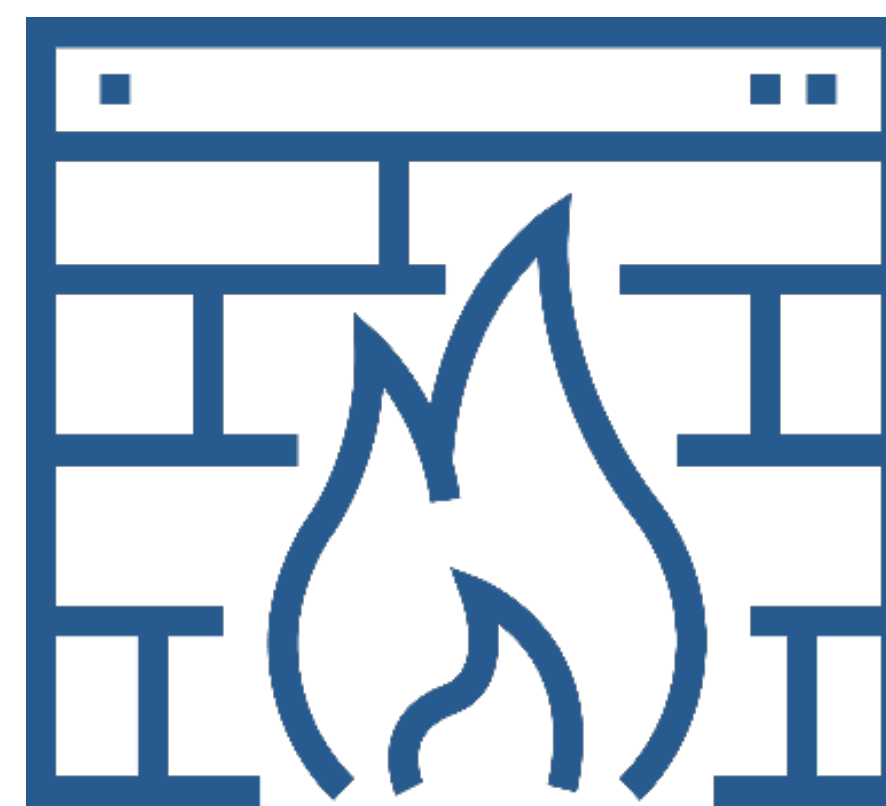
МИНПРОМТОРГ
РОССИИ

Межсетевое экранирование



Сетевая
Безопасность

- Выявление и блокировка более 2000 прикладных протоколов и приложений (DPI)
- Идентификация пользователей с использованием:
 - Microsoft Active Directory
 - Captive Portal с LDAP каталогом
- Выборочное логирование правил МЭ
- Счётчик правил МЭ





Предотвращение вторжений



Сетевая
Безопасность



ViPNet Coordinator VA

☰

Статистика и журналы ▾

Межсетевой экран ▾

Защищенная сеть (VPN) ▾

Предотвращение вторжений

Прикладные сервисы ▾

Сетевые настройки

Маршрутизация ▾

Системные настройки ▾

Предотвращение вторжений включено ✎

🔍

📁

⚙️ Параметры правил

↻ Обновление базы

📖 ▾

Блокирующие ✕

☐ Правило предотвращения	Статус	Действие
☐ "ET EXPLOIT Quanta LTE Router UDP Backdoor Activation Attempt"	🟢 Вкл	Блокировать
☐ "ET EXPLOIT Serialized Java Object Generated by ysoserial"	🟢 Вкл	Блокировать
☐ "ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli)"	🟢 Вкл	Блокировать
☐ "AM Exploit Disk Sorter Enterprise 9.1.12 Buffer Overflow exploit"	🟢 Вкл	Блокировать
☐ "AM Exploit Weblogic Remote Code Execution"	🟢 Вкл	Блокировать
☐ "AM Exploit rConfig v3.9.2 unauthenticated Remote Code Execution"	🟢 Вкл	Блокировать
☐ "AM EXPLOIT Unauthenticated XSS SugarCRM Enterprise"	🟢 Вкл	Блокировать
☐ "AM Exploit Hootoo HT-05 - RCE"	🟢 Вкл	Блокировать
☐ "AM Exploit Solr RCE stage 2"	🟢 Вкл	Блокировать



VPN с ГОСТ шифрованием



Сетевая
Безопасность

- VPN-шлюз сетевого уровня (L3 VPN)
- VPN-шлюз канального уровня (L2OverIP VPN)
- Remote Access VPN (ViPNet Client)
- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 (для обратной совместимости)
- IPsec 6 – протокол безопасности сетевого уровня

ТК 26 Р 1323565.1.034-2020 «Информационная технология.
Криптографическая защита информации. Протокол безопасности сетевого
уровня»

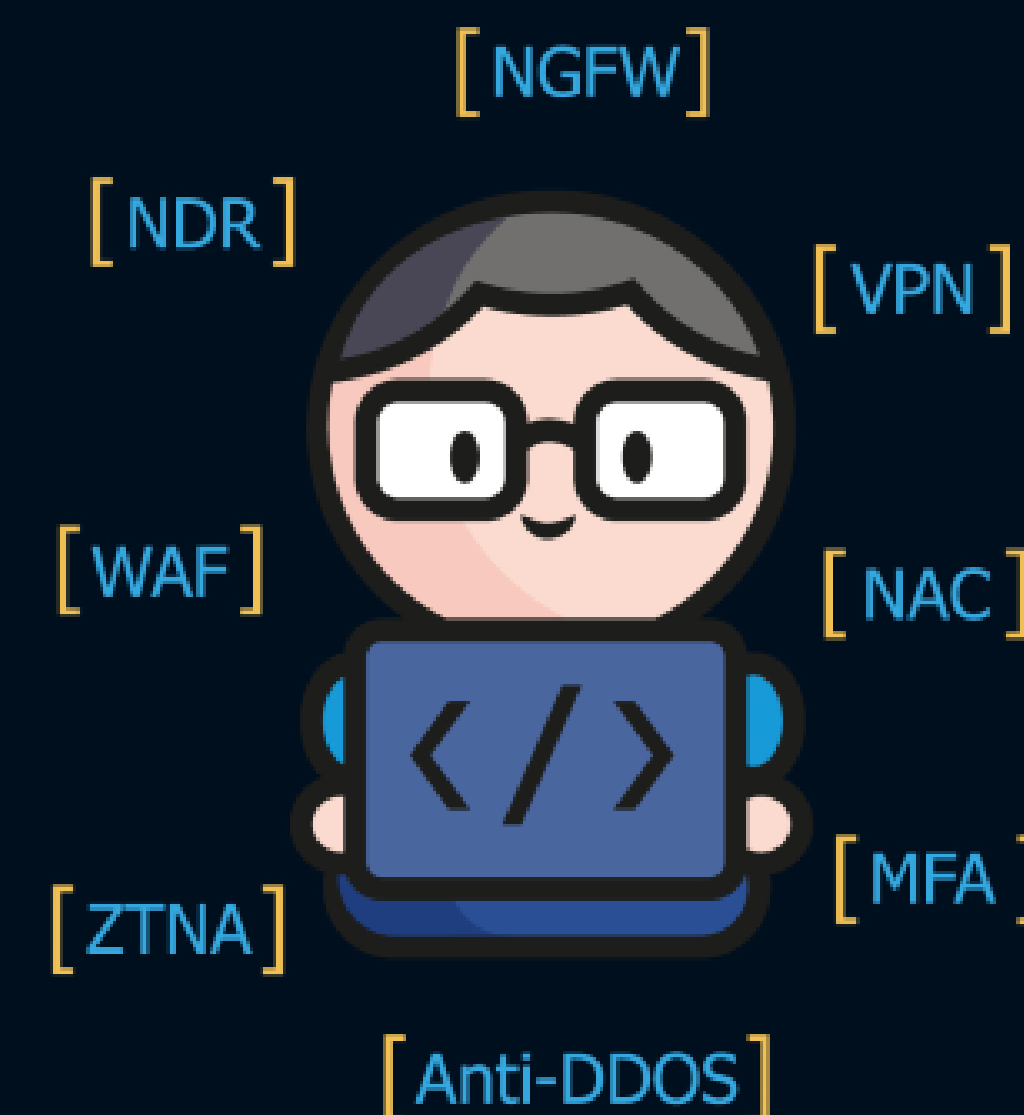


Криптографическая защита



Сетевая
Безопасность

- Защита канала управления МЭ (IPsec, TLS)
- Аутентификация администраторов
- Защита резервных копий
- Контроль целостности ПО, БРП, журналов
- Проверка обновления ПО (проверка ЭП)





Сетевые функции



Сетевая
Безопасность

- Статическая и динамическая маршрутизация (OSPF, BGP)
- Политики маршрутизации (Policy-based routing)
- Поддержка VLAN (802.1Q)
- Агрегирование сетевых интерфейсов (802.3ad)
- Поддержка Jumbo-кадров и Path MTU Discovery
- Приоритизация трафика (QoS, ToS, DiffServ)
- Встроенный DHCP-, DNS-, NTP-сервер
- ICAP, SNMPv2/v3, Syslog (CEF), SSH, HTTPS





Отказоустойчивость и резервирование



Сетевая
Безопасность

- Отказоустойчивый кластер высокой доступности
- Синхронизация таблицы соединений между элементами кластера
- Резервирование каналов связи и интерфейсов
- **Минимальное время переключения кластера сократилось до 1 секунды**





Сетевая
Безопасность

Новая система управления

ViPNet Prime

Ядро

Лицензирование
Ролевая модель
Управление ПО

VPN

Управление
структурой сети,
генерация ключей

PMM

Управление
политиками
безопасности

NVS

Мониторинг
состояния
узлов

ViPNet Coordinator HW 5



Сетевая
Безопасность

Схема лицензирования

Next-Generation Firewall

Based

Advanced

VPN

МЭ

Прокси

IPS

DPI

Лицензия может быть как бессрочной, так и срочной – подписка



Сетевая
Безопасность

Модельный ряд



HW50



HW100



Малые офисы и филиалы

HW1000

HW1000 C

HW1000 D



Предприятия среднего бизнеса

HW2000



HW5000



Крупные предприятия, ЦОД

ViPNet Coordinator VA



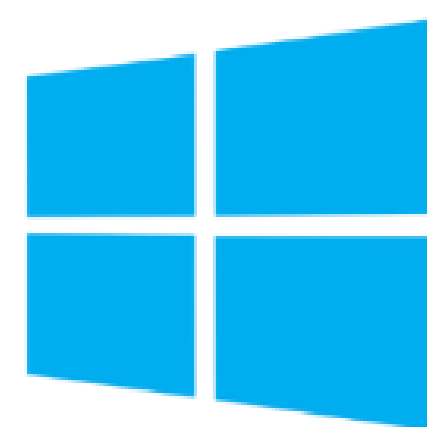
Сетевая
Безопасность

Поддерживаемые гипервизоры:

- KVM, QEMU-KVM и Libvirt
- VMware ESXi
- VMware Workstation
- Microsoft Hyper-V Server
- Oracle VM Server
- Oracle VM VirtualBox



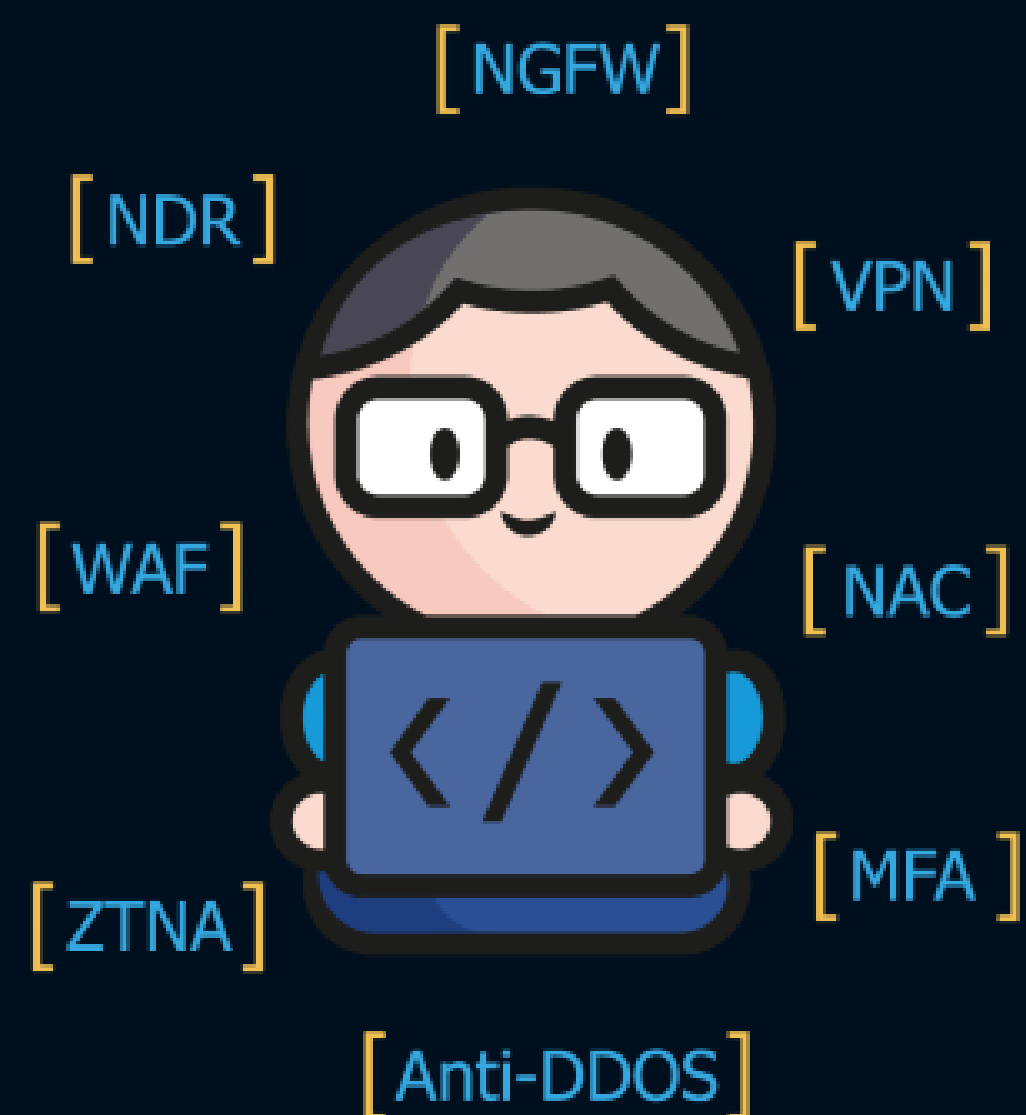
vmware®



Microsoft
Hyper-v

ORACLE®

VM
VirtualBox





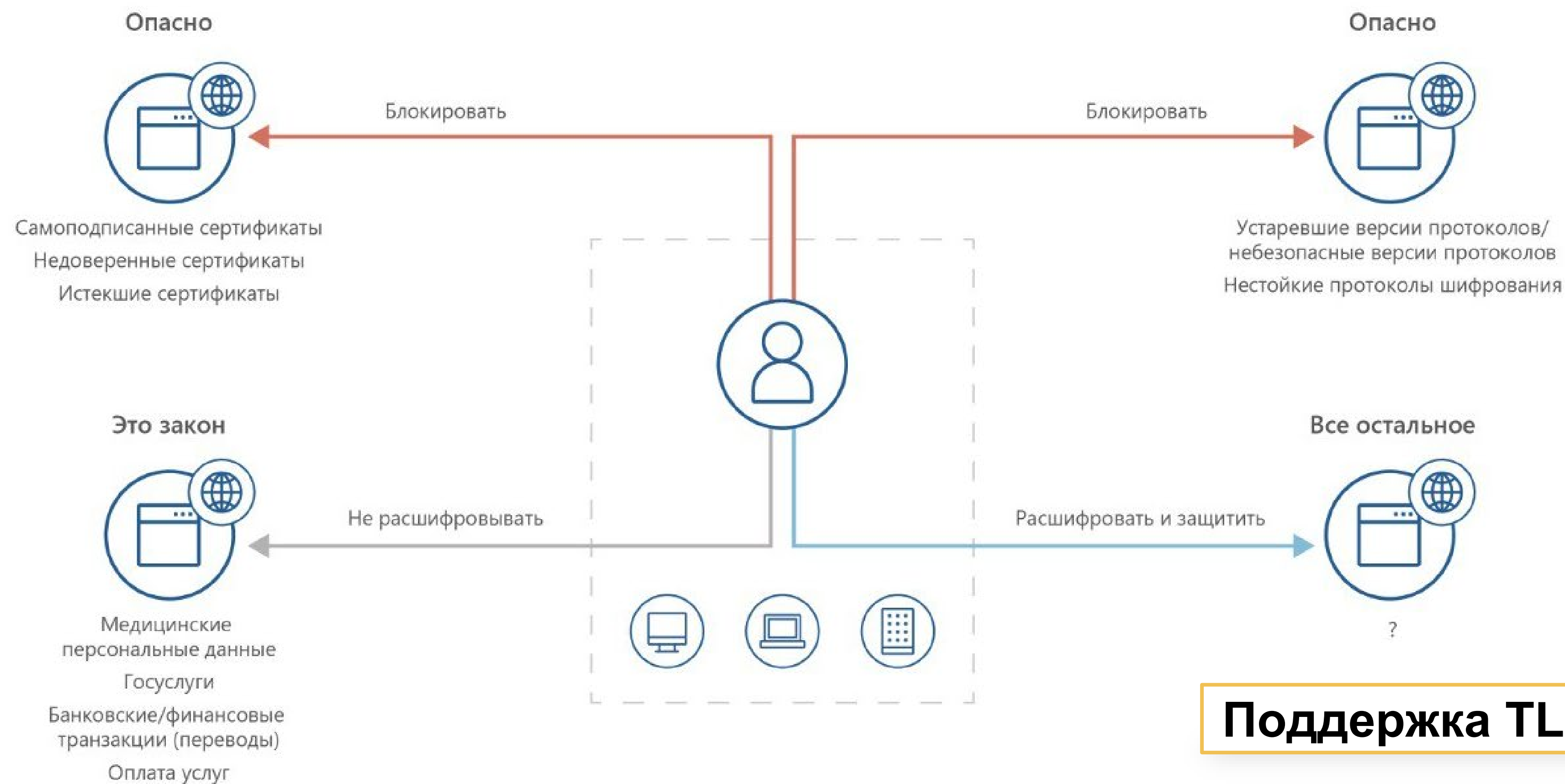
Сетевая
Безопасность

ПЛАНЫ РАЗВИТИЯ

SSL/TLS-инспекция



Сетевая
Безопасность



Поддержка TLS 1.3

URL-фильтрация



Сетевая
Безопасность

~100 млн. веб-ресурсов

80 категорий

+15% ежемесячный
прирост базы



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



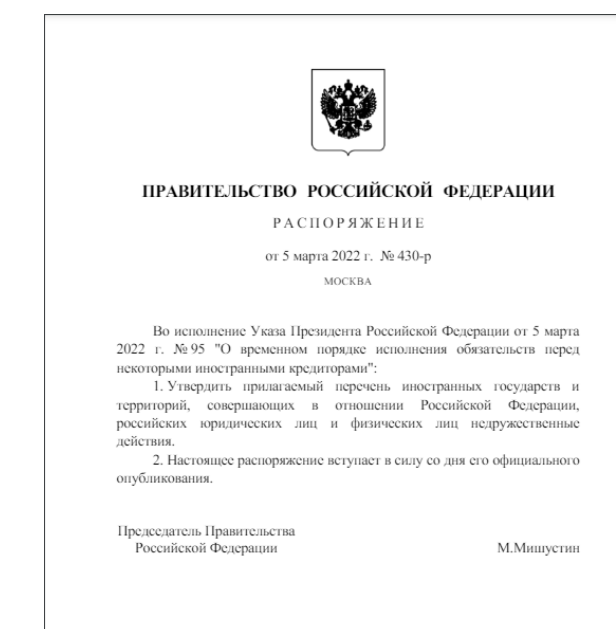
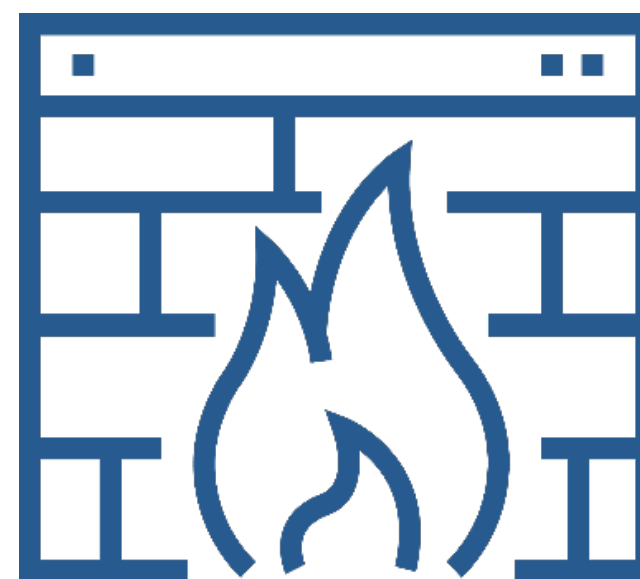


Блокировка по GEO-IP



Сетевая
Безопасность

- Фильтрация трафика на основе данных о географической принадлежности отправителей
- Использование доверенной базы геолокации IP-адресов на базе «Главного радиочастотного центра» (ФГУП «ГРЧЦ»)



Дружественные страны





Сетевая
Безопасность

Обнаружение вредоносного ПО

ViPNet Coordinator HW

Admin 99+ i

Состояние системы

Журналы

Статистика

Межсетевой экран

Защищённая сеть (VPN)

Предотвращение вторжений

Прикладные службы

Сетевые настройки

Маршрутизация

Системные настройки

Предотвращение вторжений включено

Правила IPSМетоды 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

ViPNet Coordinator HW

Admin 99+ i

Состояние системы

Журналы

Статистика

Межсетевой экран

- Сетевые фильтры
- Трансляция адресов (NAT)
- Обработка прикладных протоколов
- Группы объектов
- Прокси-сервер
- ICAP-серверы

Защищённая сеть (VPN)

Предотвращение вторжений

Прикладные службы

Сетевые настройки

Маршрутизация

Системные настройки

ICAP-серверы

Поиск + Добавить ICAP-сервер

Статус	Имя сервера	Режим и тип	Адрес и порт	Путь к ICAP-серверу	Передаваемые параметры
ON	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
ON	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
ON	Solar Dozor DLP-система Solar	Инспекция трафика Система предотвращения	192.168.1.15:1344	Исходящего: /outgoing-traffic	Выкл.
ON	ICAP-сервер	Зеркалирование трафика	192.168.15.22:1344	Входящего: /incoming-traffic	Выкл.

Инспекция:

SSL/TLS-инспекция

Предотвращение вторжений (IPS)

Обнаружение вредоносного ПО

Антивирус (av)

Песочница (sandbox)

Предотвращение утечки данных (dlp)



**Сетевая
Безопасность**

**Спасибо
за внимание!**



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363