

Next-Generation Firewall (NGFW)

Gartner®

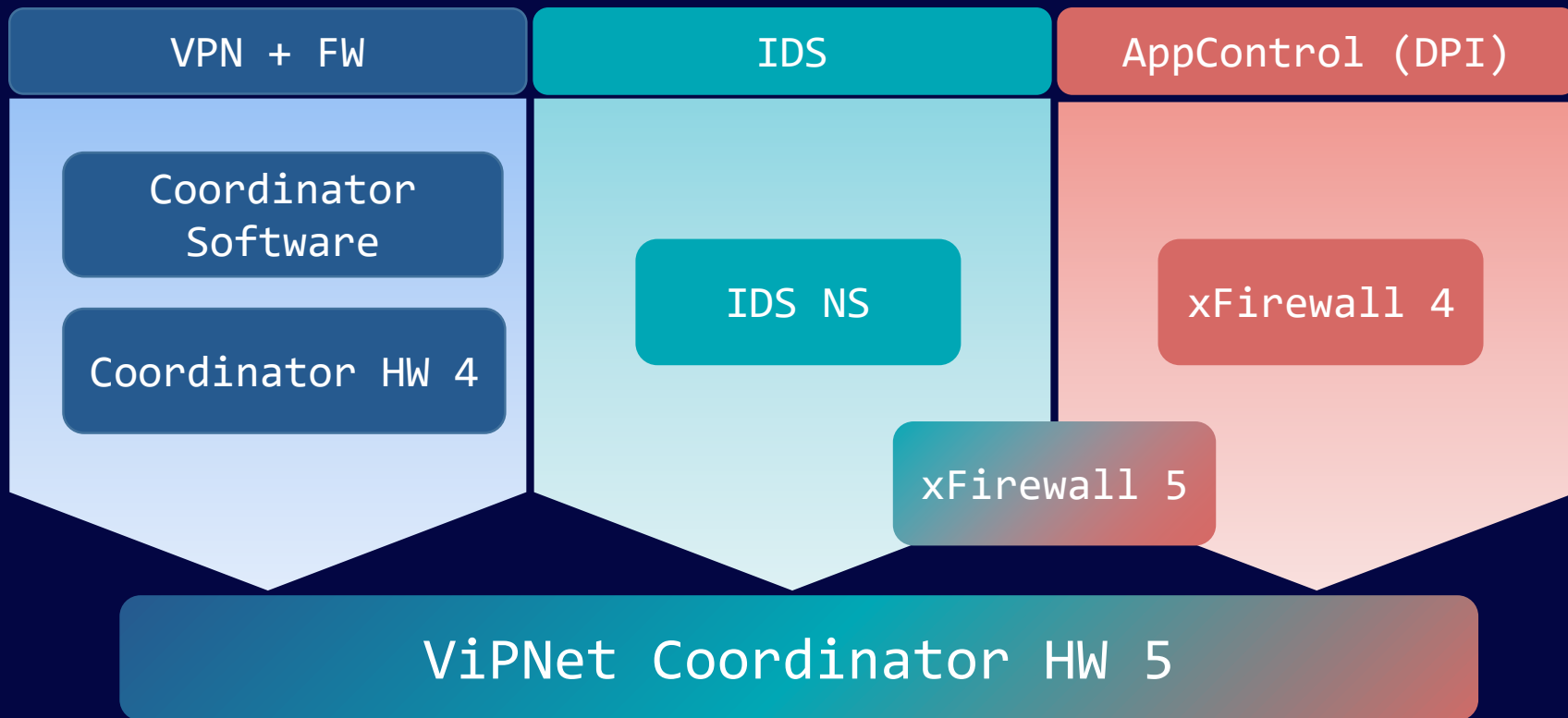
МЭ следующего поколения (NGFW) в дополнении к общепринятому разграничению доступа предоставляет возможности по выявлению и блокировке современных угроз, таких как: вредоносное ПО, атаки уровня приложений.

Согласно определению Gartner NGFW должен состоять из:

- стандартный МЭ SPI
- встроенная система IPS
- система контроля приложений
- Дополнительная информация об угрозах



Шлюзы безопасности ViPNet



Два NGFW в портфолио



xFirewall, Coordinator HW 5

ФСТЭК России

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



Coordinator HW 5

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

Минцифры России

- В реестре российского ПО

Основные модули безопасности



Application Control



IDS/IPS



VPN



**Аутентификация
пользователей**



**Фильтрация по URL
Инспектирование TLS**



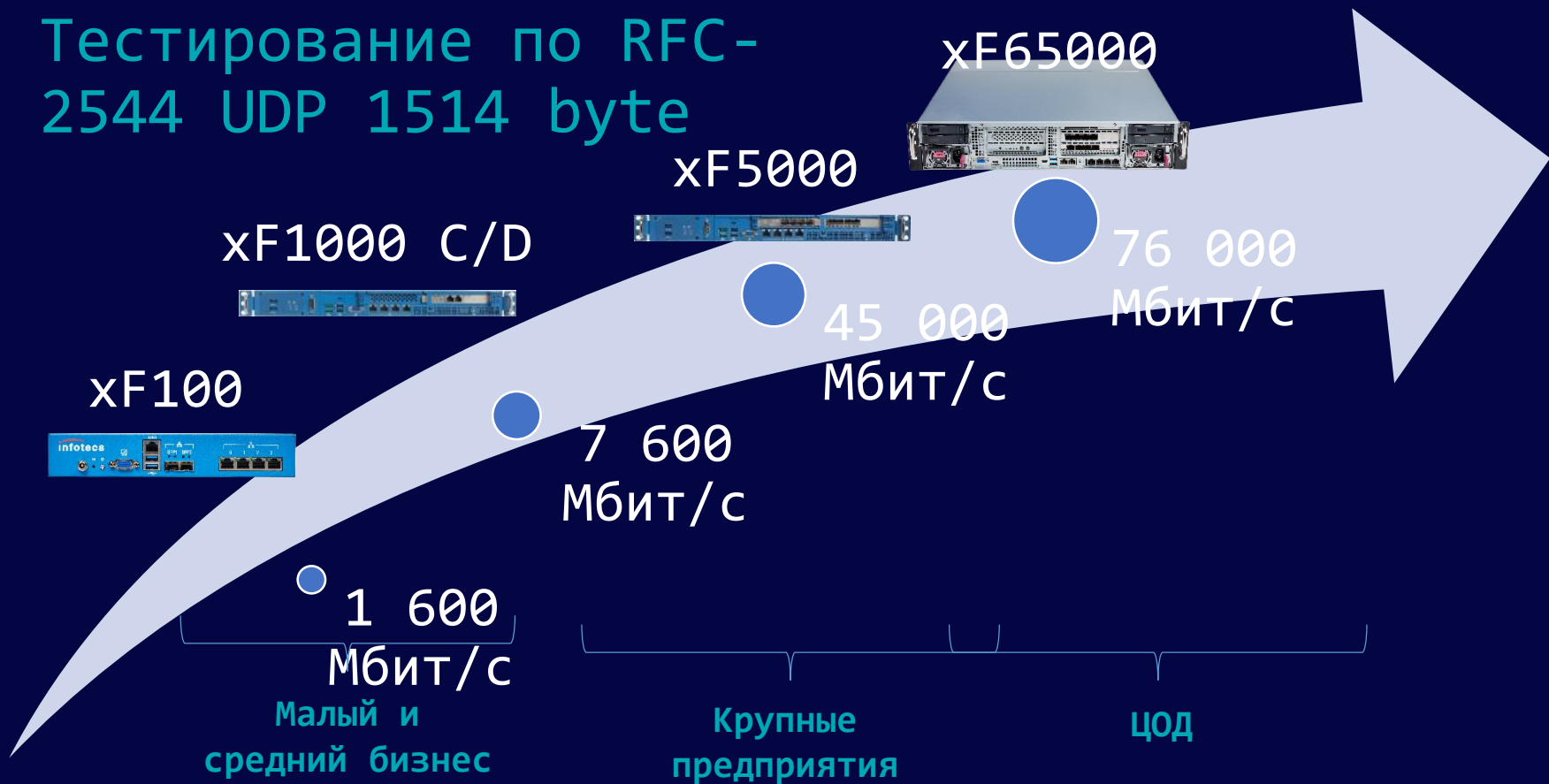
**Антивирус
Антиспам**

VIPNet xFirewall 5



Модельный ряд xFirewall

Тестирование по RFC-
2544 UDP 1514 byte

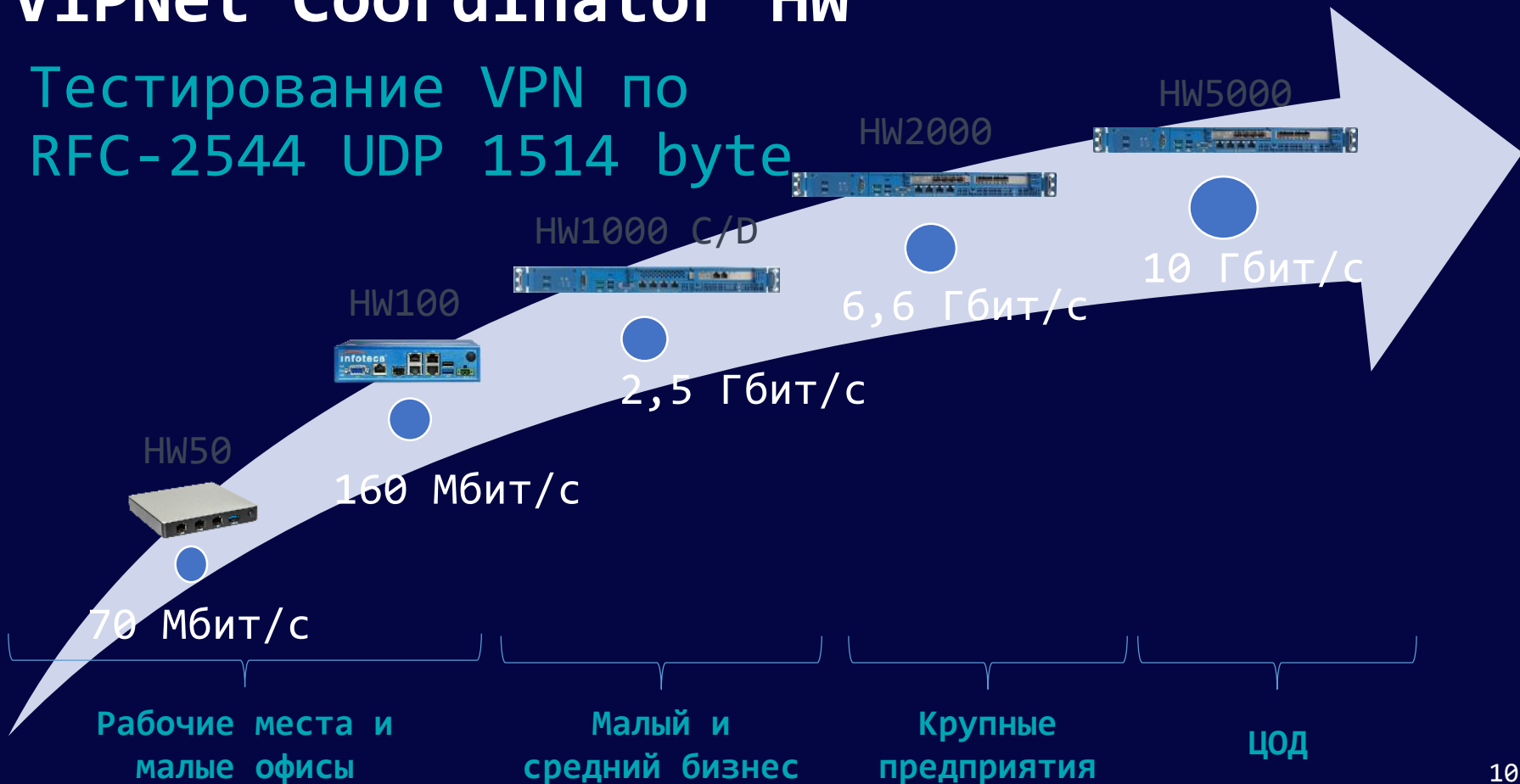


VIPNet Coordinator HW 5



VIPNet Coordinator HW

Тестирование VPN по
RFC-2544 UDP 1514 byte



Что нового в 5.6.4

1

Улучшенный
механизм SSL/TLS-
инспекции

2

Расширение
возможностей
агрегированных
интерфейсов

3

Улучшенный
пользовательский
интерфейс

4

Поддержка новых
аппаратных платформ

Что нового в 5.6.4

5

RADIUS-аутентификация
для SSH-подключений

6

Сброс к заводским
настройкам

7

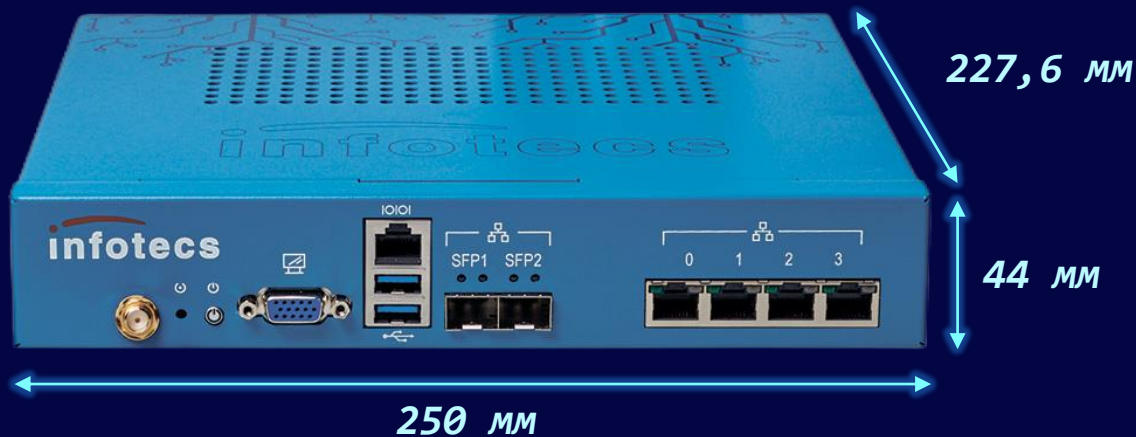
Повышена скорость
и стабильность отправки
CEF-сообщений

8

Исправление
ошибок



xF100 Q1/Q2



6 сетевых интерфейсов:

- 4 x 1 Гбит/сек RJ45
- 2 x 1 Гбит/сек SFP



Незначительно повысилась производительность

Производительность

Исполнение	xF100 N1	xF100 Q1/Q2
Firewall, 1518 Байт UDP (Мбит/сек)	722	1 600
Firewall, TCP Multistream (Мбит/сек)	600	1 380
AppControl (Firewall+DPI), (Мбит/сек)	180	395
NGFW (FW+DPI+IPS) (Мбит/сек)	13	40
NGFW+SSL Inspection (1МБ)	32	50
Firewall Throughput (UDP 64 Байт)	79 000	137 000
Connections per Second	10 000	18 000
Concurrent Connections	149 993	499 994

Производительность

Исполнение	xF1000 Q7/Q8	xF5000 Q2
Firewall, 1518 Байт UDP (Мбит/сек)	7 600	51 000
Firewall, TCP Multistream (Мбит/сек)	11 000	33 000
AppControl (Firewall+DPI), (Мбит/сек)	2 600	7 800
NGFW (FW+DPI+IPS) (Мбит/сек)	480	1 300
NGFW+SSL Inspection (1МБ)	480	1 300
Firewall Throughput (UDP 64 Байт)	2 200 000	4 000 000
Connections per Second	53 000	106 000
Concurrent Connections	4 999 000	29 999 990

Radius - аутентификация

- Чтобы пользователь подключался к ViPNet xFirewall в режиме администратора, установите значение атрибута shell:priv-lvl равным 15.
- При другом значении атрибута shell:priv-lvl или при его отсутствии подключение будет выполняться в режиме пользователя.

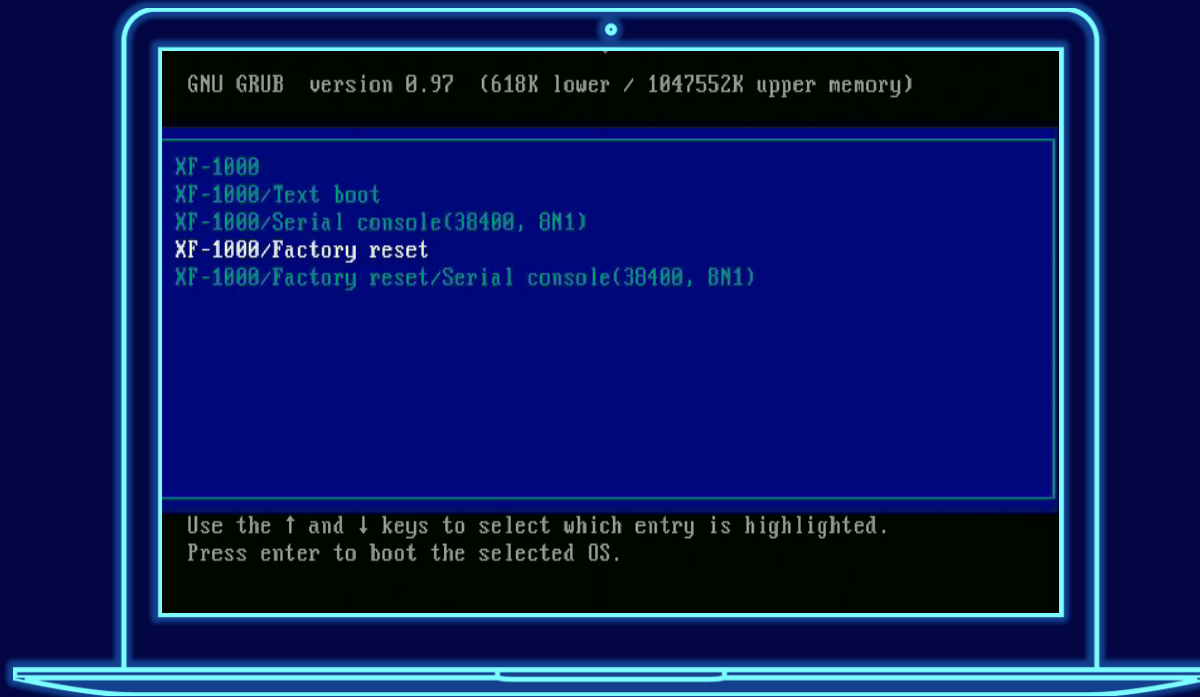


Возможность возврата к предыдущей версии ViPNet xFirewall



В ViPNet xFirewall добавлена возможность возврата ПО к версии 5.4.0

Сброс к заводским настройкам



В строке Are you sure you want to execute this command and delete key? Введите Delete нажмите Enter.

Улучшения SSL Inspection

SSL/TLS-инспекция

Общие настройки Исключения

SSL-сертификат

Общие сведения

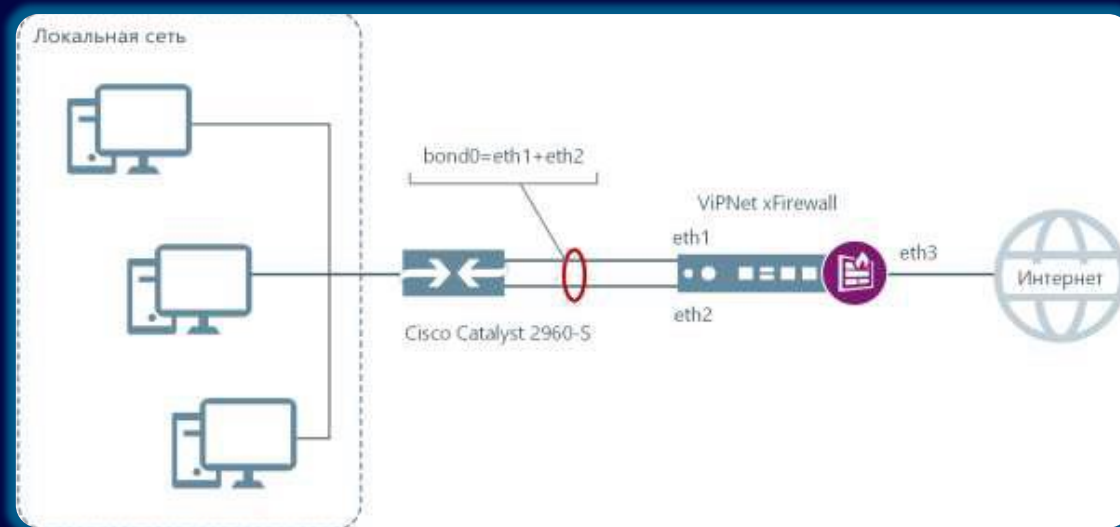
Субъект: xfva-1a06000c
Срок действия: 22.11.2028
Издатель: xfva-1a06000c
Имя файла: ssl_decryption_cert.pem
Серийный номер: ebde8353e52a890e

Криптографические параметры

Разрешенные протоколы: SSL 3, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3
Алгоритмы обмена ключами: RSA, ECDHE, DHE
Алгоритмы шифрования: 3DES, RC4
Алгоритмы аутентификации: MD5, SHA1, SHA256, SHA384

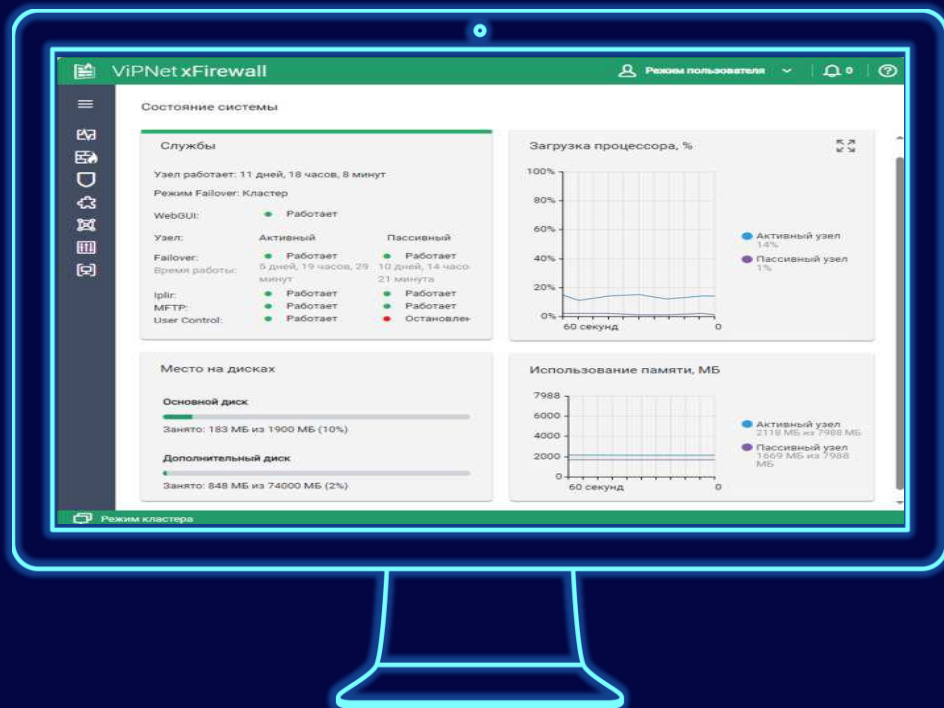
- Добавлена поддержка расшифровывания протокола TLS 1.3
- Добавлена возможность инспекции трафика HTTP/2
- Добавлены настройки доверия к сертификатам ресурсов:
 - проверка срока действия сертификатов;
 - проверка полей сертификата, определяющих его использование (key usage, extended key usage);
 - проверка самоподписанных сертификатов.
- Исключать из инспекции веб-ресурсы, используя их альтернативные имена (SAN – Subject Alternative Names) и поддомены (wildcard).

Агрегация интерфейсов



- Ранее вы могли включать в состав агрегированного интерфейса только до трех подчиненных физических. Теперь это ограничение снято.
- Максимальное количество агрегированных интерфейсов увеличено до 8.

Изменен вывод контролируемых параметров



Теперь отображается относительная загрузка CPU, а максимальная загрузка всех ядер принята за 100%.

VIPNet xFirewall Add-ons

GeoIP

Модуль
устанавливается
самостоятельно
Заказчиком.

Назначение –
блокировка
трафика по Гео-
признакам.

Используется база
ГРЦ.

Принципы GeoIP-фильтрации трафика



Модуль GeoIP-фильтрации

Модуль VipNet xFirewall, позволяющий разграничивать доступ на основе геолокации. Блокирует входящий трафик из заданных регионов.



Первый этап анализа трафика

Это снижает долю трафика, анализируемого DPI, IPS, что повышает эффективность межсетевого экрана.



Белый список

Можно исключить из GeoIP-фильтрации отдельные IP-адреса или подсети.



Next

Прошедший GeoIP-фильтрацию трафик обрабатывается другими подсистемами межсетевого экрана.

VIPNet xFirewall xF65000 Межсетевой экран для защиты ЦОДов



Исполнение xF65000



- 2U платформа производства Аквариус
- 4 x 1Gb RJ-45
- 4 x 1Gb SFP
- 8 x 10Gb SFP+
- 2 БП

Новые возможности

1

**Высокая
производительность**
85 тыс. правил
DPI+IPS без деградации

2

HA-Cluster
Синхронизация сессий
Переключение за 1 сек

3

**Динамическая
маршрутизация**
BGP
OSPF

4

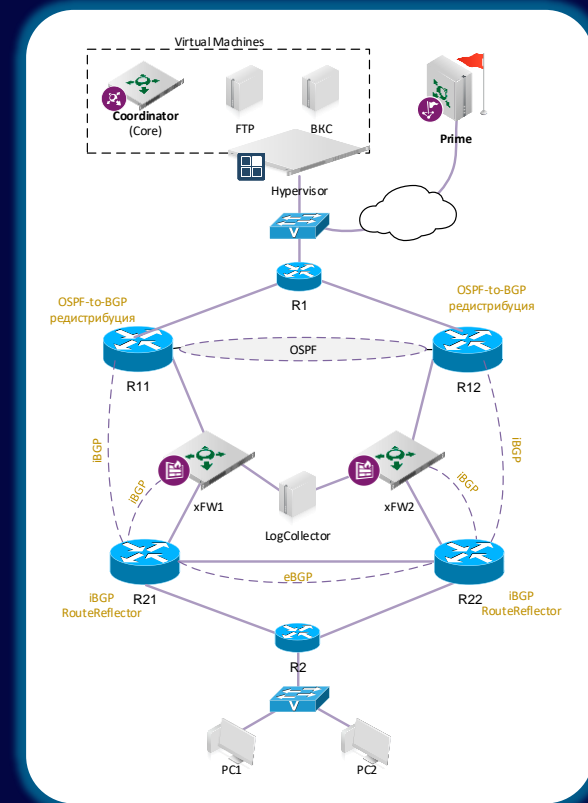
Шлюзовой антивирус
Прокси-сервер
Поддержка ICAP

5

Резервирование
2 блока питания
Поддержка BFD

BGP. Моделирование переключения кластера

- Отключение питания активной ноды xFW1
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер ВКС\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился
- Включение питания активной ноды xFW 2
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер ВКС\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился



Сравнение производительности

Checkpoint 28000



Firewall

145 Гбит/сек

Next Gen Firewall

51,5 Гбит/сек

ViPNet xFirewall xF65000



Firewall

76 Гбит/сек

Next Gen Firewall

60 Гбит/сек

Требования по сертификации

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
- Многофункциональный межсетевой экран уровня сети **NEW**



Минцифры России

- В реестре российского ПО

VPN с ГОСТ шифрованием



- 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) **NEW**
- ГОСТ 28147-89 для обратной совместимости
- IPsec 6 – протокол безопасности сетевого уровня **NEW**

Многофункциональный МЭ



Аппаратные платформы

HW50



HW100



Малые офисы и филиалы

HW1000

HW1000 C

HW1000 D



Предприятия среднего
бизнеса

HW2000



HW5000



Крупные предприятия,
ЦОД

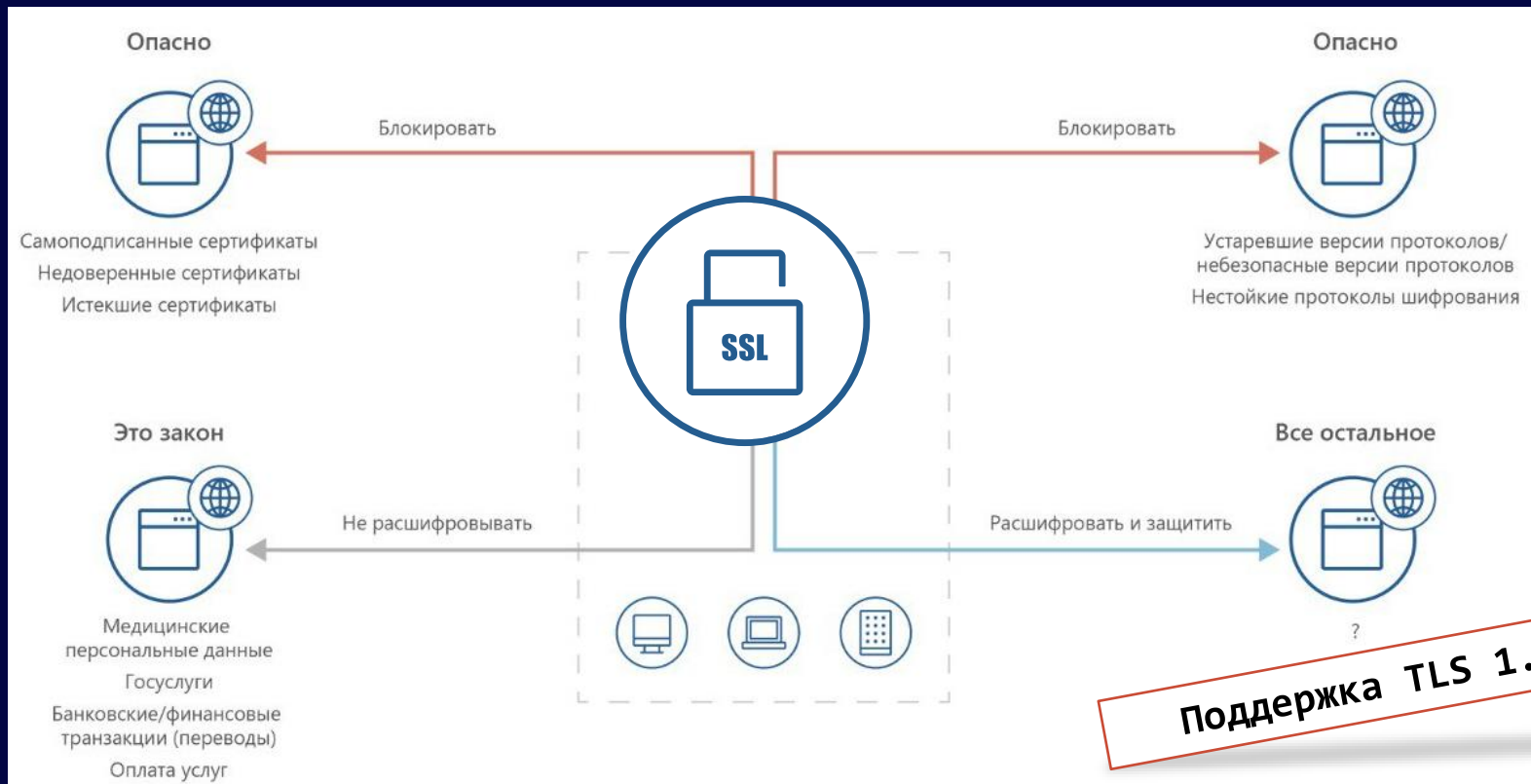
VIPNet Coordinator HW 5.4/5.5

- SSL/TLS-инспекция
- URL-фильтрация
- Блокировка по GEO-IP
- Встроенный антивирус
- Проверка состояния связи между шлюзами
- Локальные учетные записи + новая роль
- Интеграция VIPNet SafeBoot



Идет сертификация

SSL/TLS-инспекция



Поддержка TLS 1.3

Источник баз URL-категорий

~100 млн веб-ресурсов

80 категорий

+15% ежемесячный
прирост базы



URL-фильтрация

Межсетевой экран ^

- Сетевые фильтры
- Трансляция адресов (NAT)
- Группы объектов
- ISAP-сервер
- Пользователи сети
- Расшифровка SSL/TLS
- Прикладные службы v
- Сетевые настройки v
- Системные настройки v
- Управляющие соединения

База URL-категорий

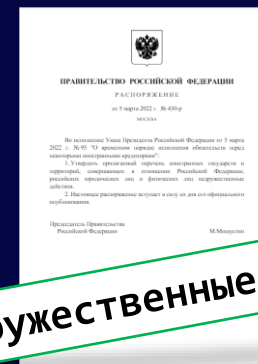
Обновить v | Настройки обновления с сервера

Поиск... | + Добавить | Импортировать | Всего: 33

<input type="checkbox"/> Имя URL-категории	Состав	Описание
<input type="checkbox"/> Настраиваемые (2)		
<input type="checkbox"/> Категория 1	activation.sls.microsoft.com messenger.live.com lr.live.net account.live.com update.microsoft.com	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt
<input type="checkbox"/> Категория 1	account.live.com	
<input type="checkbox"/> Из базы URL-категорий (27)		
Malware	3581 веб-ресурс	Сайты, распространяющие вирусы и
Phishing & Typosquatting	4984 веб-ресурсов	Фишинг и регистрация доменных имён,
Botnets & C2C	8916 веб-ресурсов	Ботнеты и командные центры для их
Реклама и баннеры	1233 веб-ресурса	Сайты рекламных и баннерных сетей или
Наркотики	3219 веб-ресурсов	Сайты, рекламирующие или продающие
Грубость, матерщина, непристойность	3219 веб-ресурсов	Сайты, содержащие избыточное количество

Блокировка по GEO-IP

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



Блокировка по GEO-IP

The screenshot shows the ViPNet Coordinator HW web interface. The top navigation bar includes a search bar, navigation arrows, and a refresh button. The main header displays the system name 'ViPNet Coordinator HW' and the user 'Admin' with a notification bell showing '99+'.

The left sidebar contains a menu with the following items:

- Состояние системы
- Журналы
- Статистика
- Межсетевой экран
 - Сетевые фильтры
 - Трансляция адресов (NAT)
 - Обработка прикладных протоколов
 - Группы объектов**
 - Прокси-сервер
 - Пользователи сети
- Защищённая сеть (VPN)
- Предотвращение вторжений
- Прикладные службы
- Сетевые настройки
- Маршрутизация

The main content area is titled 'Группы объектов' and has several tabs: Узлы ViPNet, IP-адреса, Интерфейсы, Протоколы, Расписания, and **Страны**. Below the tabs is a search bar and a button 'Обновить из файла'. A table lists countries with their flags and codes:

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

The right sidebar shows the details for 'Антигуа и Барбуда'. It includes a section 'Список применений группового объекта' with the note 'Объект не используется' and a section 'Общая информация' showing 'Страна: Антигуа и Барбуда' and 'Код: AG'. There is also a link for 'Список подсетей'.

Локальные учетные записи

ViPNet _BRAND_NAME_ | xfva-3306000c

GeneralAdmin | 99+ | i



Статистика и журналы ^

Межсетевой экран ^

Прикладные службы ^

Сетевые настройки ^

Системные настройки ^

Общие

Сертификаты

Сервисные функции

Учётные записи

Управляющие соединения

Учётные записи

Локальные учётные записи | Активные сеансы

+ Добавить

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

Обнаружение вредоносного ПО

The screenshot shows the ViPNet Coordinator HW web interface. The top navigation bar includes the title 'ViPNet Coordinator HW', a user profile 'Admin', a notification bell with '99+', and an information icon. A left sidebar contains a menu with items like '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 has two tabs: 'Правила IPS' and 'Методы анализа'. Under 'Методы анализа', there are two configuration cards. The first card, 'База правил IPS', shows the database release date as 'от 27 мая 2021, 15:00', the update server as 'updateids.infotecs.ru', and the expiration date as '13 мая 2022, 03:00'. The second card, 'Обнаружение вредоносного ПО', shows the database release date as 'от 27 мая 2021, 15:00', the update server as 'updatemd.infotecs.ru', and the expiration date as '13 мая 2022, 03:00'. Both cards include 'Обновить базу' and 'Настройки обновления с сервера' options.

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 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



infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети



https://vk.com/infotecs_news



https://t.me/infotecs_news