

ViPNet xFirewall 5 и 6 поколения – когда нужно реально импортозаместить NGFW

Алексей Данилов
руководитель продуктового направления

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  ФЕСТ

Новые возможности версии 5.6.4

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

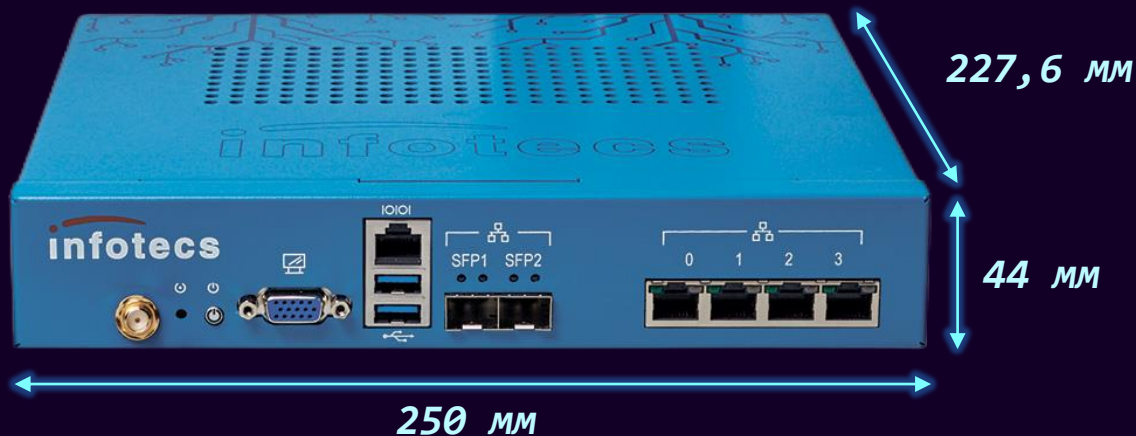
Повышена скорость
и стабильность отправки
CEF-сообщений

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.

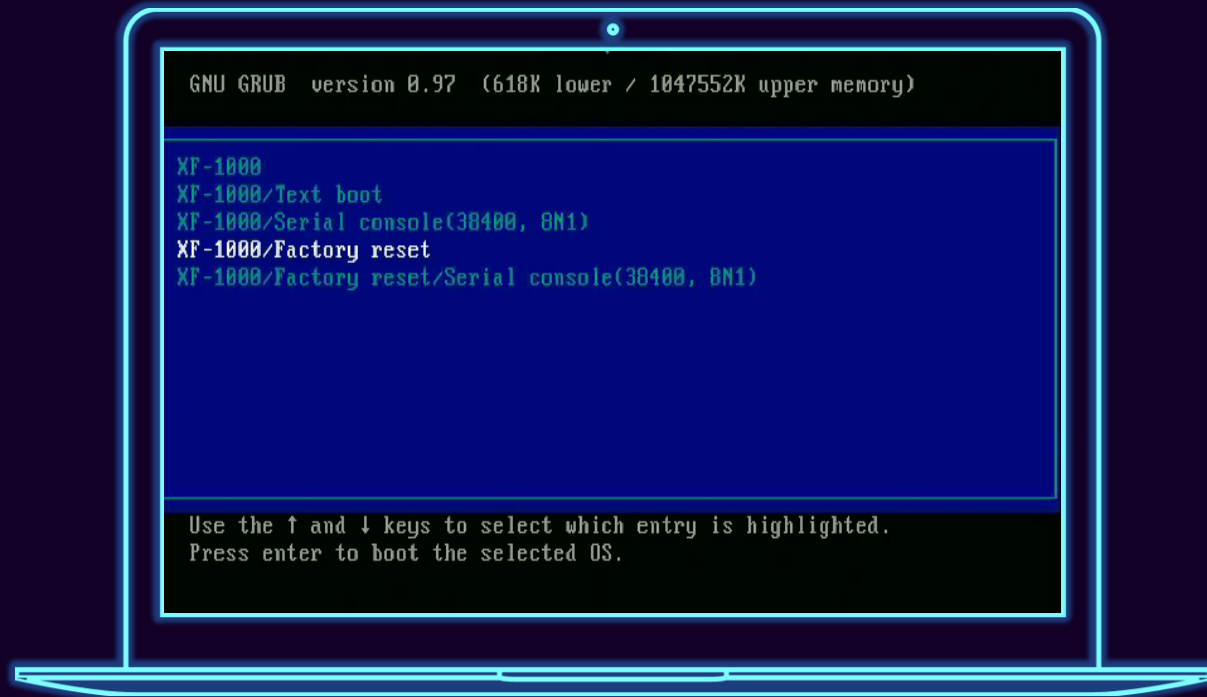


Возможность возврата к предыдущей версии ViPNet xFirewall



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

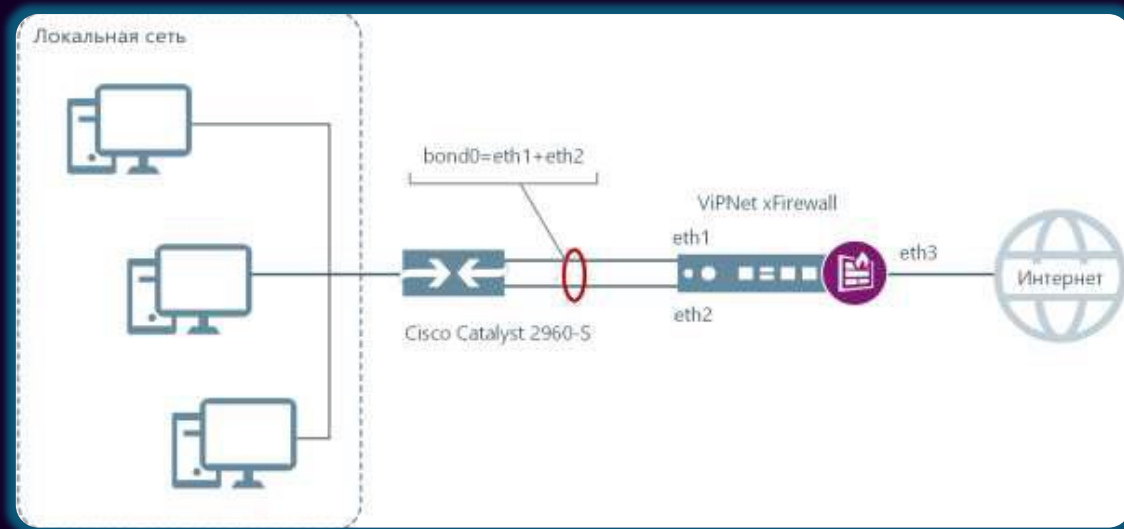
Субъект: xfva-1a06000c
Срок действия: 22.11.2028
Издатель: xfva-1a06000c
Имя файла: ssl_decryption_cert.pem
Серийный номер: ebde8353e52a890e

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

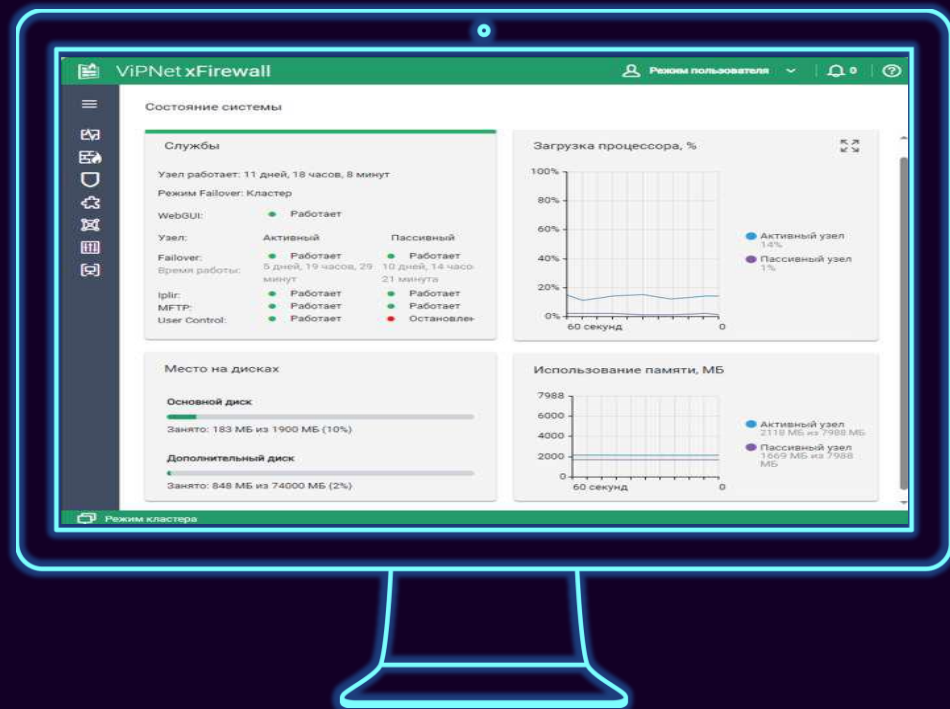
- Добавлена поддержка расшифровывания протокола TLS 1.3
- Добавлена возможность инспекции трафика HTTP/2
- Добавлены настройки доверия к сертификатам ресурсов:
 - проверка срока действия сертификатов;
 - проверка полей сертификата, определяющих его использование (key usage, extended key usage);
 - проверка 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
ГРЧЦ.

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

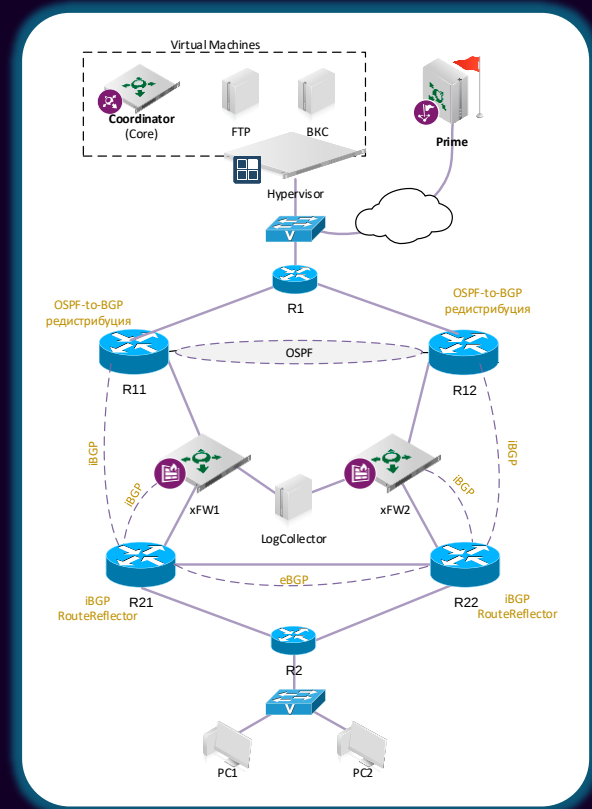
Шлюзовой антивирус
Прокси-сервер
Поддержка ICAP

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

Тестирование по требованиям заказчика

Условия тестирования

Протокол/Приложение	Порт	Доля Throughput, %
HTTPS	TCP/443	32,26
SMB/CIFS (MS DS)	TCP/445	30,48
HTTP	TCP/80	5,37
Citrix	TCP/1494	6,94
RDP	TCP/3389	1,4
DNS	UDP/53	0,3
SNMP	UDP/161	1
Syslog	UDP/514	6,89
MS SQL	TCP/1433	9,7
Имитация VNC	TCP/8080	5,66

Проведенные тесты

Номер теста	Характеристика набора правил				Ожидаемая пропускная способность, не менее, Гбит/с	Зафиксированы результаты, Гбит/с
	Количество правил, не менее	Срабатывающее правило	IPS	DPI		
1	85 000	все	нет	да	20	22
2	85 000	все	да	да	10	12
3	85 000	последнее	нет	да	20	22
4	85 000	последнее	да	да	10	12



График теста №1



График теста №2

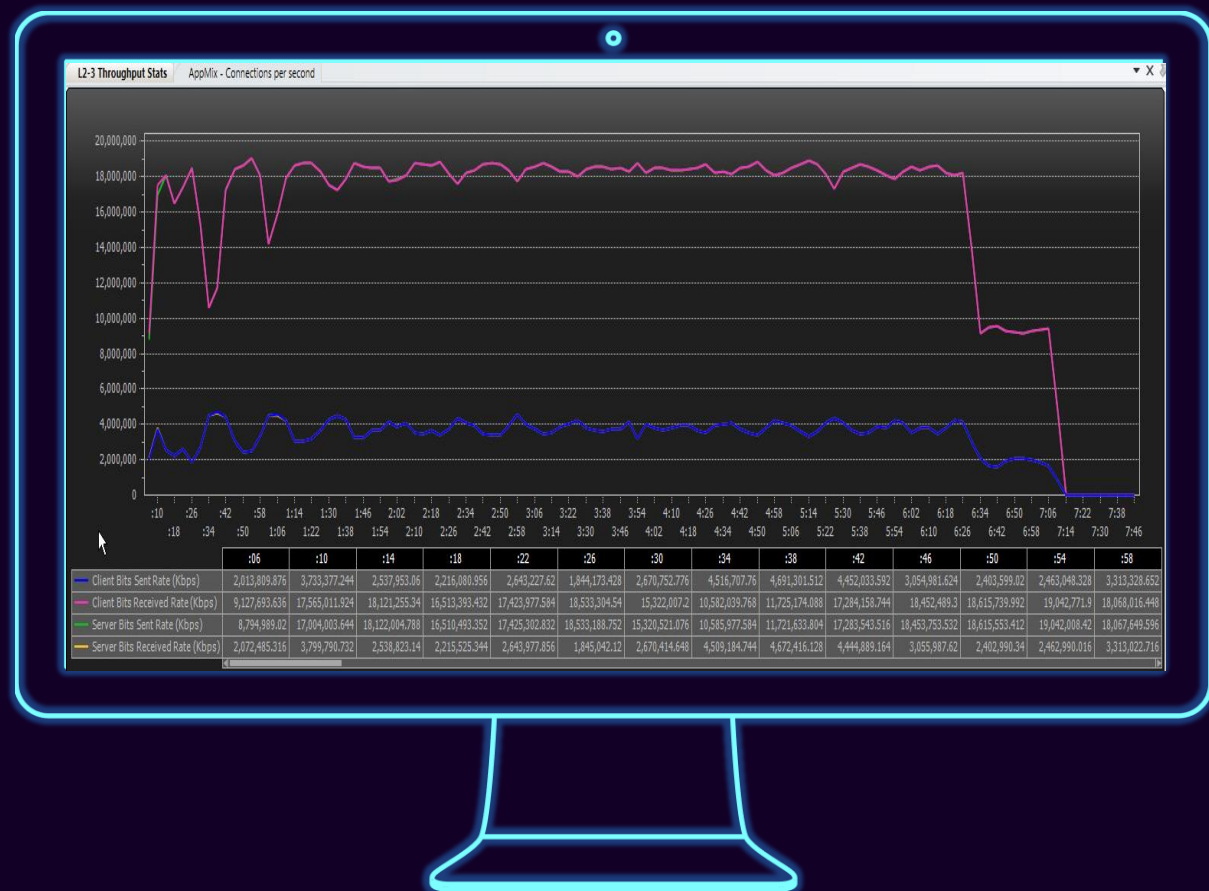


График теста №3

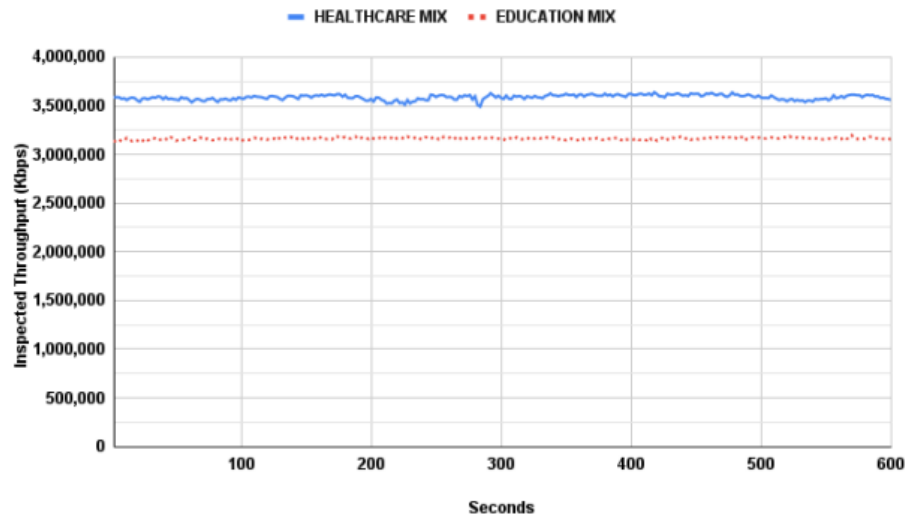


График теста №4

Обратите внимание

Это норма

Inspected Throughput Sustained Phase



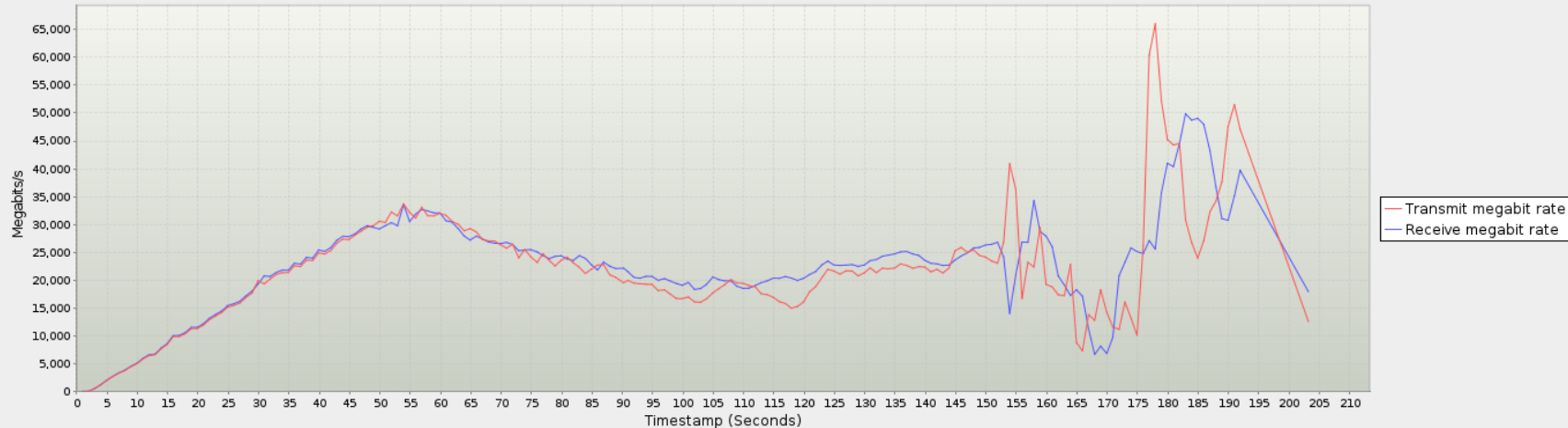
Согласно RFC-9411, длительность теста должна быть не менее 300 секунд, без учета процесса «разгона» нагрузчика.

NetSecOPEN Certification Network Security Product
Performance Testing Cisco Secure Firewall 3105



- Весь тест длился 205 секунд
- Из них 50 секунд стенд разгонялся
- Результаты колеблются от 7 до 70 Гбит/сек
- У теста нет стабильности

7.22.2 : Application Data Throughput



ViPNet xFirewall 6.0.0

Основные возможности 6 поколения

1

Standalone лицензия
Активация серийного
номера через Интернет

2

**Повышение
производительности**
В 6-10 раз зависит
от теста

3

**Динамическая
маршрутизация**
BGP
OSPF на базе FRR модуля

4

HA-Cluster
Синхронизация L7-
сессий, переключение
без перерыва сервисов

5

**Новые NGFW
функции**
GeoIP, URL,
Antivirus...

Первый релиз 6.0.0

Бета-версия – 19.12.2025



Обновление с xF 5 поколения на xF 6 поколения (локальное)



Обновление xF 6 поколения с версии 6.0.0 на последующие с помощью webUI



Новая ролевая модель



Экспорт/импорт индивидуальной конфигурации ПАК



Экспорт/импорт универсальной конфигурации ПАК



Сброс к заводским настройкам через GRUB

Общесистемные возможности

Первый релиз 6.0.0

Продолжение



Передача журналов
(системных, пакетов)
в множество систем,
поддержка протокола tcp



Доработка отправки
статистики по протоколу
Netflow v9 во внешние
системы



Возможность
аутентификации
по протоколу radius



Удаленное получение
логов с резервной ноды



Ввод серийного номера
ПАК в ходе эксплуатации
для инвентаризации



Расширение параметров
мониторинга здоровья

Общесистемные возможности

Первый релиз 6.0.0

Продолжение



Поддержка BGP,
OSPF на базе FRR



Поддержка
аутентификации в OSPF



Обнаружение недоступных
шлюзов (DGD) на FRR



Политики маршрутизации
(PBR) на FRR



Расширенная маршрутизация

Первый релиз 6.0.0

Продолжение



Повышение производительности для 85 тыс. правил для исполнений xF5000, xF65000



Реализация нового журнала ip-пакетов – журнала сессий



Выборочное журналирование для правил доступа



Запись IP-пакета в рсар по срабатыванию сигнатуры БРП



Использование профилей сигнатур IPS (mobile, Workstations, SCADA, VoIP и т.д.)



Потоковый Антивирус

Общесистемные возможности

ТЕХНО infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

