




# ViPNet xFirewall

Межсетевой экран  
НОВОГО ПОКОЛЕНИЯ



Программно-аппаратный комплекс (ПАК) ViPNet xFirewall – это шлюз безопасности, сочетающий функции традиционного межсетевого экрана с расширенными функциями анализа и фильтрации трафика, устанавливается на границе сети, предназначен для комплексного решения задач информационной безопасности в корпоративных сетях, позволяет создать гранулированную политику безопасности на основе учетных записей пользователей и списка приложений и обеспечивает обнаружение и нейтрализацию сетевых вторжений.

## ПРЕИМУЩЕСТВА



Гранулированная политика безопасности, которая строится в терминах «Пользователь» - «Приложение» - «разрешить/запретить»



Обеспечение безопасного использования персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BYOD (Bring Your Own Device)



Выявление и блокировка более 2000 прикладных протоколов и приложений: игры, социальные сети, torrent и т. д.

- Снижение расходов на потребление интернет-трафика
- Минимизация поверхности атак



Обнаружение и нейтрализация сетевых вторжений с использованием встроенной системы предотвращения вторжений (IPS). Совместно с решением ViPNet TDR (Threat Detection and Response) позволяет:

- Сократить среднее время обнаружения инцидента с 30 до 2 минут по сравнению с ручным анализом событий
- Снизить затраты на эксплуатацию системы обнаружения вторжений
- Упростить реагирование на угрозы ИБ

# ВОЗМОЖНОСТИ

## МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ УРОВНЯ ПРИЛОЖЕНИЙ (DPI – DEEP PACKET INSPECTION)

Выявление и блокировка более 2000 прикладных протоколов и приложений среди которых:

- игры
- социальные сети
- сервисы мгновенных сообщений
- видео трансляции
- сервисы P2P, torrent
- хостинг файлов
- туннелирование, VPN
- удаленное управление
- промышленные протоколы

## МЕЖСЕТЕВОЙ ЭКРАН

- Межсетевой экран с контролем состояния сессий
- Трансляция адресов NAT/PAT
- Защита от атак Antispoofing

## СЕТЕВЫЕ ФУНКЦИИ

- Развитая статическая маршрутизация
- Динамическая маршрутизация
- Поддержка VLAN (dot1q)
- Агрегирование каналов связи (bonding (LACP), EtherChannel)
- Поддержка QoS, ToS, DiffServ

## СЕРВИСНЫЕ ФУНКЦИИ

- DNS-сервер
- NTP-сервер
- DHCP-сервер
- DHCP-Relay

## ОТКАЗОУСТОЙЧИВОСТЬ И РЕЗЕРВИРОВАНИЕ

- Кластер горячего резервирования – failover
- Поддержка ИБП (UPS)

## ИНТЕГРАЦИЯ С КАТАЛОГАМИ СПРАВОЧНИКОВ

- Microsoft AD
- Captive Portal с LDAP-каталогом

## DPI (DEEP PACKET INSPECTION)

Механизм глубокой инспекции протоколов. DPI использует различные техники идентификации трафика пользовательских приложений: на основе портов и протоколов, сигнатурный метод, эвристический метод. Эти подходы позволяют выявить даже те приложения, трафик которых шифруется или маскируется.

## ПРОКСИ СЕРВЕР

- Поддержка протокола HTTP
- Проверка и фильтрация трафика по MIME-типу файлов и по типу HTTP-метода запроса
- Проверка трафика сторонним антивирусом, подключаемым по протоколу ICAP

## СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IPS – INTRUSION PREVENTION SYSTEM)

- Сигнатурный метод анализа трафика
- Эвристический метод анализа трафика
- База правил, содержащая описания сетевых угроз, регулярно обновляется специалистами ОАО «ИнфоТекС» для поддержания в актуальном состоянии

При обнаружении характерных признаков вторжения (срабатывании правила IPS) возможны следующие действия с IP-пакетом:

- IP-пакет блокируется межсетевым экраном ViPNet xFirewall
- IP-пакет пропускается для дальнейшей обработки с предупреждением

Экспорт зарегистрированного события в систему ViPNet TIAS из решения ViPNet TDR с целью выявления и предотвращения инцидентов.

## Производительность<sup>1</sup>

Исполнение	xF100	xF1000 C/D	xF5000
МЭ, 1518 байт UDP (Мбит/сек) <sup>2</sup>	800	2 700	19 000
МЭ (пакетов/сек)	90 000	1 300 000	4 000 000
МЭ, TCP (Мбит/сек)	720	2 700	9 300
Application Control (МЭ+DPI) <sup>3</sup> (Мбит/сек)	190	1 900	7 100
NGFW Throughput <sup>4</sup> (Мбит/с)	9,5	249	669
Соединений в секунду	2 500	20 000	50 000
Количество одновременно обслуживаемых соединений	148 500	990 000	9 900 000

## Аппаратные характеристики

Наименование аппаратной платформы	xF100	xF1000 C/D	xF5000
Форм-фактор	ПАК (MiniPC)	ПАК (19' Rack 1U)	ПАК (19' Rack 1U)
Размеры (Ш x В x Г)	170 x 41,5 x 138 мм	430 x 43,4 x 380 мм	444 x 44 x 383 мм
Масса	1 кг	7,2 кг	13 кг
Источник питания	DC 24В; 2,5А	Встроенный БП, 110-240 В, 250 Вт	Встроенный БП, 110-240 В, 500 Вт
Порты ввода/вывода	1x VGA 2x USB	2x VGA 1x PS/2 1x COM DB9 6x USB	1x VGA 1x PS/2 KB/Mouse port 1x COM DB9 2x USB
Сетевые порты	4 x RJ45 1 Гбит/с 1 x SFP 1 Гбит/с	HW1000 C: 6 x RJ45 10/100/1000 Мбит/с  HW1000 D: 4 x RJ45 10/100/1000 Мбит/с 2 x SFP 10/100/1000 Мбит/с	4 x RJ45 1 Гбит/с 4 x SFP+ 10 Гбит/с

<sup>1</sup>Производительность зависит от активированных функций, характеристик обрабатываемого сетевого трафика: протоколов, размера пакетов. Производительность может меняться вследствие изменений, вносимых в новые версии программного обеспечения.

<sup>2</sup>Результаты получены на основании методики ОАО «ИнфоТекС»

<sup>3</sup>Результаты получены для трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

<sup>4</sup>Результаты получены для активированных МЭ, DPI, IPS с использованием актуальной на момент теста базы правил IPS, при анализе трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

## СЕРТИФИКАЦИЯ

### ФСТЭК РОССИИ

Ведутся работы с целью подтверждения сертификатов соответствия требованиям:

- «Профиль защиты межсетевого экрана 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)
- «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ»



📍 ОАО «ИнфоТекС», 127287, Москва,  
Старый Петровско-Разумовский пр-д, 1/23, стр. 1

✉ soft@infotecs.ru  
hotline@infotecs.ru

☎ +7 495 737-61-92  
8 800 250-0-260 (бесплатный звонок по России)

🌐 www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в ОАО «ИнфоТекС». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы ™ или ® в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.