infotecs

ViPNet xFirewall

Межсетевой экран нового поколения (NGFW)

ПАК ViPNet xFirewall – это шлюз безопасности – межсетевой экран нового поколения, сочетающий функции классического межсетевого экрана: анализ состояния сессии, проксирование, трансляция адресов; с расширенными функциями анализа и фильтрации трафика такими как: глубокая инспекция протоколов, выявление и предотвращение компьютерных атак, инспекция SSL/TLS-трафика, взаимодействие с антивирусными решениями, DLP и песочницами.

ViPNet xFirewall 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, обеспечивает обнаружение и нейтрализацию сетевых вторжений.

ВОЗМОЖНОСТИ

МЕЖСЕТЕВОЙ ЭКРАН

Межсетевой экран с контролем состояния сессий

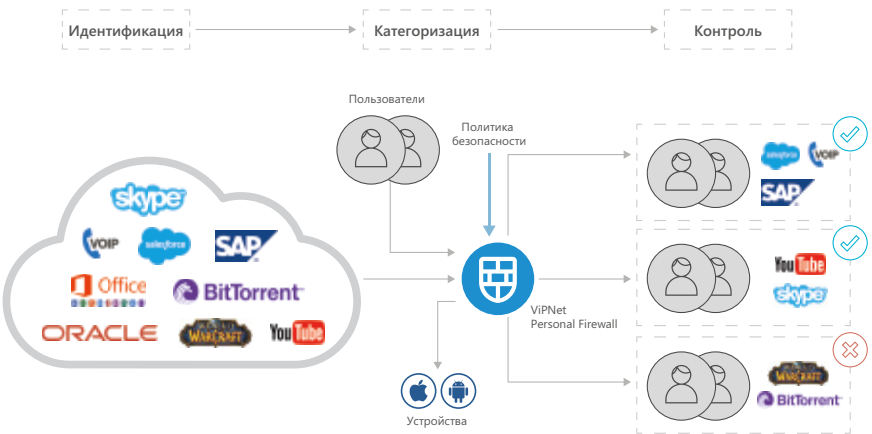
Трансляция адресов NAT/PAT

Защита от атак Antispoofing

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ УРОВНЯ ПРИЛОЖЕНИЙ – ГЛУБОКАЯ ИНСПЕКЦИЯ ПРОТОКОЛОВ (DPI – DEEP PACKET INSPECTION)

Выявление и блокировка более 5000 прикладных протоколов и приложений, среди которых:

- Игры
- Социальные сети
- Сервисы мгновенных сообщений
- Видеотрансляции
- Сервисы P2P, torrent
- Хостинг файлов
- Туннелирование, VPN
- Удаленное управление
- Промышленные протоколы



DPI (deep packet inspection) – механизм глубокой инспекции протоколов. DPI использует различные техники идентификации трафика пользовательских приложений на основе портов и протоколов, сигнатурного и эвристического методов.

[ПРОИЗВОДИТЕЛЬНОСТЬ][1]

Исполнение	xF100	xF1000 C/D	xF5000
			
МЭ, 1518 байт UDP (Мбит/сек)[2]	800	2 700	19 000
МЭ (пакетов/сек)	90 000	1 300 000	4 000 000
МЭ, TCP (Мбит/сек)	720	2 700	9300
Application Control (МЭ+DPI)[3] (Мбит/сек)	190	1 500	3 400
NGFW Throughput[4] (Мбит/с)	9,5	249	669
NGFW+SSL Inspection[5] (Мбит/с)		260	615
Соединений в секунду	2 500	20 000	50 000
Кол-во одновременно обслуживаемых соединений	148 500	990 000	9 900 000

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

[2]Результаты получены на основании методики АО «ИнфоТеКС»

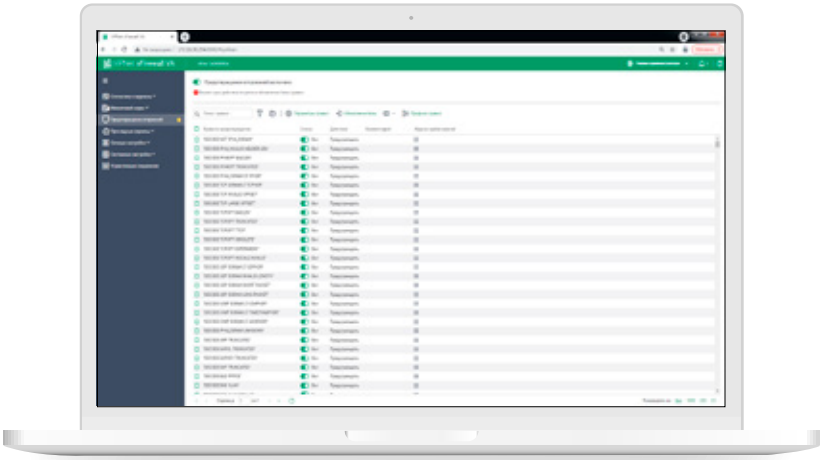
[3]Результаты получены для трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

[4]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.

[5]Результаты получены для активированных МЭ, DPI, IPS с использованием актуальной на момент теста базы правил IPS, контентной и антивирусной инспекции SSL-трафика при анализе HTTPS-трафика.

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IPS – INTRUSION PREVENTION SYSTEM)

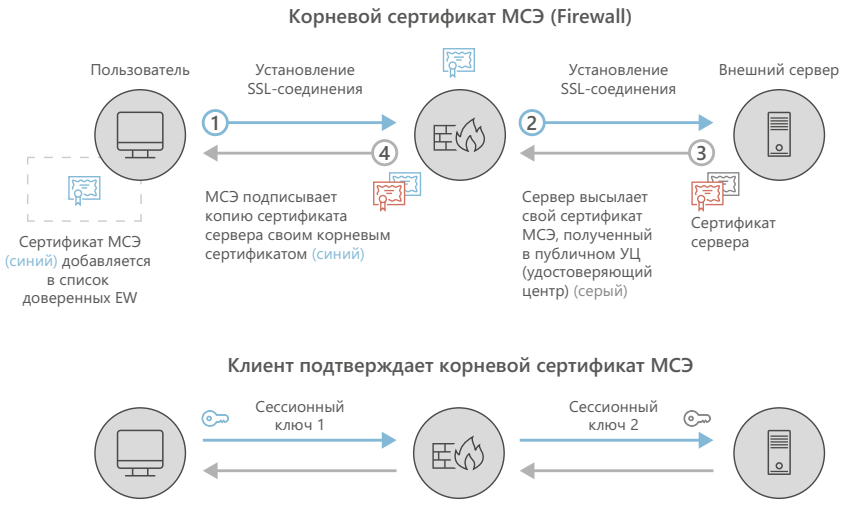
- Сигнатурный метод анализа трафика
- Эвристический метод анализа трафика
- Актуальная база правил, содержащая описания сетевых угроз, регулярно обновляемая специалистами ИнфоТеКС



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

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

ИНСПЕКЦИЯ SSL/TLS-ТРАФИКА



- Классификация SSL/TLS-трафика, выявление и выборочная фильтрация трафика приложений
- Исследование содержимого SSL/TLS-сессий средствами DPI и IPS
- URL- и контент-фильтрация HTTP(S)-трафика
- Выявление и блокировка вирусов и вредоносного ПО в HTTP(S)-трафике

Инспекция SSL/TLS подразумевает два шага:

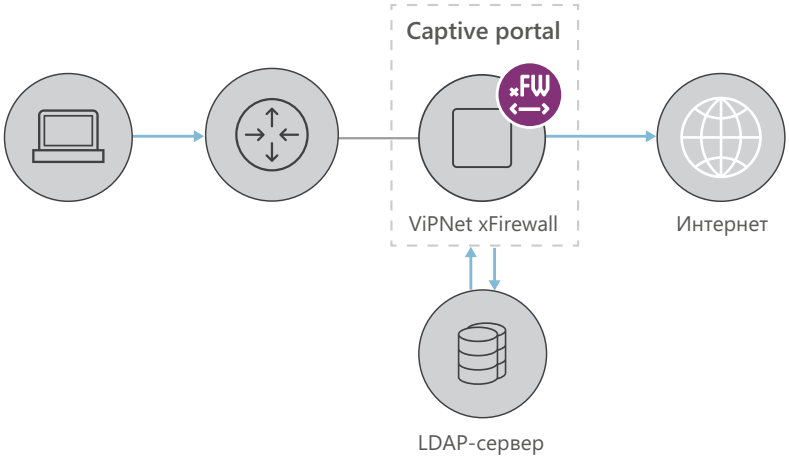
1) SSL decryption – расшифровывание SSL-трафика, проходящего через межсетевой экран

2) Анализ содержимого SSL-трафика

Расшифровывание SSL-трафика в ViPNet xFirewall реализовано по принципу проксирования – forward proxy decryption. Все стадии этого процесса схематично изображены на рисунке выше.

ИНТЕГРАЦИЯ С КАТАЛОГАМИ СПРАВОЧНИКОВ

- Microsoft AD
- Captive Portal с LDAP каталогом



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)

[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)

Инспекция SSL/TLS-трафика средствами глубокой инспекции протоколов, системой предотвращения атак, антивирусными решениями и контентной фильтрацией

[АППАРАТНЫЕ ХАРАКТЕРИСТИКИ]

Наименование аппаратной платформы	xF100 N1	xF1000 Q7, Q8	xF5000 Q2
			
Форм-фактор	ПАК (MiniPC)	ПАК (19’ Rack 1U)	ПАК (19’ Rack 1U)
Размеры (Ш × В × Г), мм	170 x 41,5 x 138	430 x 43,4 x 380	444 x 44 x 383
Масса, кг	1	7,2	7,9
Источник питания	DC 24В; 2,5А	xF1000 Q7 – встроенный БП, 110-240 В, 300 Вт xF1000 Q8 – два встроенных БП с функцией «горячей» замены, 110-240 В, 300 Вт	Два встроенных БП с функцией «горячей» замены, 110-240 В, 300 Вт
Порты ввода/вывода	1x VGA 2x USB	1x VGA 1x COM DB9 6x USB	1x VGA 1x COM DB9 6x USB
Сетевые порты	• 4 x RJ45 1 Гбит/с • 1 x SFP 1 Гбит/с	xF1000 Q7: • 8 x RJ45 10/100/1000 Мбит/с xF1000 Q8: • 4 x RJ45 10/100/1000 Мбит/с • 4 x SFP 10/100/1000 Мбит/с	• 4 x RJ45 1 Гбит/с • 8 x SFP+ 10 Гбит/с

[СЕРТИФИКАЦИЯ]

ФСТЭК РОССИИ

Соответствует:

- «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия
- «Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профилю защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016)
- «Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профилю защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016)
- «Требованиям к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профилю защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012)

infotecs

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

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

CHP22_00RU

ViPNet Virtual Private Network