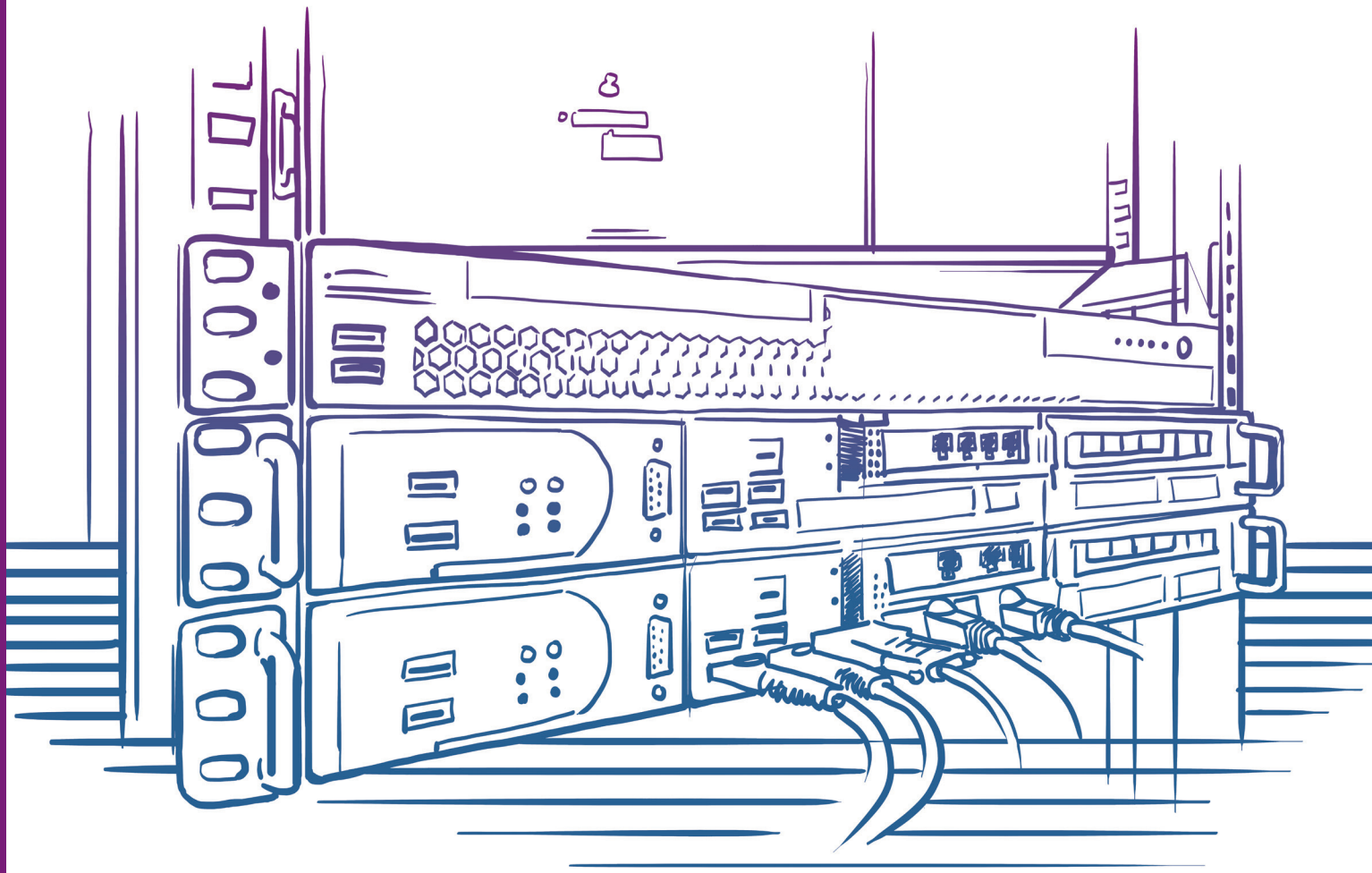
инфотекс

ViPNet xFirewall xF65000

Межсетевой экран для защиты ЦОД –
Data Center Firewall



ПАК ViPNet xFirewall xF65000

ViPNet xFirewall xF65000 – это шлюз безопасности, межсетевой экран нового поколения, сочетающий функции классического межсетевого экрана:

- анализ состояния сессии
- 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 xF65000 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.

Что такое межсетевой экран для ЦОД

ПОТРЕБНОСТИ ЦОД

Производительность

С точки зрения информационной безопасности ЦОД является уникальным объектом, потому что в нем сосредоточены все сервисы и данные компании, что представляет интерес для злоумышленников и тем самым он является важнейшим объектом, требующим защиты.

Особенностью ЦОД являются информационные потоки и сетевая топология. Информационные потоки ЦОД принято разделять на два типа North-South и East-West. North-South информационные потоки описывают взаимодействие ЦОД с пользователями, сервисами, другими словами данные виды информационных потоков отвечают за взаимодействие ЦОДа с внешним миром. East-West информационные потоки описывают взаимодействие различных сервисов и служб внутри ЦОДа.

Классической задачей межсетевого экрана является контроль трафика, входящего и выходящего из сети организации, поэтому межсетевой экран устанавливается на границе сети, его принято называть периметровым межсетевым экраном.

Применительно к задачам защиты ЦОД периметровый межсетевой экран выполняет задачу контроля информационных потоков North-South. Но в условиях ЦОД этого недостаточно, так как есть еще информационные потоки East-West, которые также необходимо контролировать. East-West информационные потоки существенно отличаются как по качеству, так и по количеству от North-South потоков. East-West информационные потоки представляют собой трафик взаимодействия серверов, СХД и сетевого оборудования между собой. Что касается объемов то по разным оценкам East-West трафик составляет до 80% всех информационных потоков в ЦОД, в то время как North-South не превышает 20%. В этой связи для контроля такого трафика нужен еще более производительный межсетевой экран.

1. **Firewall**
   76 Гбит/сек
2. **Next Gen Firewall**
   13 Гбит/сек*
3. **L3 new Connection**
   364 000 соединений/сек
4. **Max CC Connection**
   30 000 000 соединений**

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

**Ограничение средства генерации и измерения.

Эффективная защита

Прозрачность / Visibility

При обеспечении безопасности ЦОД необходимо обеспечить прозрачность всех происходящих процессов, для этого требуется реализовать контроль за деятельностью пользователей, устройств, сетей, приложений, рабочих нагрузок и процессов. Она может ускорить обнаружение атак и облегчить выявление злоумышленников, пытающихся украсть конфиденциальные данные или нарушить работу.

Прозрачность помимо повышения эффективности защиты, облегчает обнаружение узких мест в производительности, что позволяет оптимизировать процессы в ЦОД и прогнозировать его развитие. Прозрачность, помимо облегчения контроля, также сокращает время реагирования на инциденты и помогает в расследовании инцидентов.

Сегментация / Segmentation

Сегментация позволяет локализовать и остановить продвижение злоумышленников/ распространение атаки по инфраструктуре ЦОДа. Многие атаки направлены на получение прямого доступа к системе, чтобы скомпрометировать ее через уязвимости в приложениях, незащищенные порты или атаки типа «отказ в обслуживании» (DoS). Защититься от такого типа атак на 100% практически невозможно, но сегментация - ценный инструмент, позволяющий замедлить действия хакера и дать командам безопасности время для выявления проблемы, ограничения воздействия и реагирования на атаку.

Оптимальный профиль защиты

Разные системы требуют разных средств защиты и разных подходов. Для примера, периметровые межсетевые экраны в офисах предназначены для защиты клиентов от угроз, исходящих из сети Интернет, и контроль доступа к нежелательному контенту, в то время как в ЦОДа требуется защита серверов.

Для защиты ЦОД требуется:

1. **SDP**
   Разграничение доступа с учетом разумной необходимости и достаточности

2. **IPS**
   Обнаружение и предотвращение компьютерных атак, использования вредоносного ПО и эксплуатации уязвимостей

3. **Идентификация пользователей**
   Синхронизация с контроллерами доменов
   Captive Portal синхронизированный с LDAP-каталогами

4. **AppControl (DPI)**
   Более 5000 протоколов и приложений

SDP (Software-defined perimeter)

Программно-определяемый периметр – это подход к разграничению доступа, основанный на Прозрачности и Сегментации. Он позволяет на логическом уровне создать для каждого пользователя доступ к ресурсам посредством разрешенных протоколов.

IPS (Intrusion Prevention System)

Обнаруживает и предотвращает активность вредоносного или нежелательного ПО, компьютерные атаки, попытки эксплуатировать уязвимости. В случаях Zero-day-уязвимостей, сигнатуры IPS можно использовать как виртуальные патчи, которые позволяют выявлять эксплойты до тех пор, пока не будут устранены уязвимости в ПО.

Используются сигнатуры от компании «Перспективный мониторинг», входящей в группу компаний ИнфоТеКС.

«Перспективный мониторинг» – отечественная компания, на регулярной основе разрабатывающая экспертные данные для множества СЗИ.

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Для актуализации базы решающих правил мы ежемесячно анализируем до 100 000 образцов вредоносного кода и различных индикаторов компрометации, исследуем инструментарий злоумышленников и разрабатываем системы аналитики и приоритизации информации об угрозах, в результатечего каждый месяц подключаем до 1500 новых сигнатур AM Rules, которые учитывают российскую специфику атак.

Отказоустойчивость

Высокая доступность

Высокая доступность – это концепция организации отказоустойчивости системы за счет избыточности и сведения к минимуму времени простоя в случае сбоя. Избыточность достигается за счет объединения двух устройств в единый комплекс – кластер.

Сведение к минимуму времени простоя достигается за счет того, что одно из устройств кластера – активное, постоянно синхронизирует свое состояние на пассивное (резервное) по специально выделенному каналу резервирования.

Пассивное устройство отслеживает состояние активного и мгновенно переходит в активный режим в случае сбоя.

Маршрутизация

Центры обработки данных и сети, требующие высокой доступности и быстрого восстановления после сбоев, нуждаются в чрезвычайно быстром обнаружении сбоев, которое обеспечивает протокол BFD.

Протокол BFD (bidirectional forward detection) распознает сбой между двумя маршрутизаторами. Обнаружение сбоев с помощью BFD происходит очень быстро по сравнению с мониторингом соединения или частыми динамическими проверками состояния маршрутизации, такими как пакеты Hello или keepalive, используемыми в BGP, что позволяет ускорить процесс выявления сбоя и переключиться на резервный канал практически мгновенно.

1 **Резервирование каналов связи**
Поддержка протоколов динамической маршрутизации BGP, OSPF совместно с BFD

2 **Failover**
Мгновенное выявление сбоя и переключение на резервное устройство

3 **Резервное питание**
2 блока питания

4 **HA-Cluster**
Синхронизация таблицы состояния сессий с активного устройства на резервное

СЕРТИФИКАЦИЯ

ФСТЭК России № 4501
Сертификат удостоверяет, что программно-аппаратный комплекс ViPNet xFirewall 5, является программно-аппаратным средством защиты от несанкционированного доступа к информации, реализующим функции межсетевого экрана и системы обнаружения вторжений.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

xF65000 Q1

Производительность[1]

МЭ, 1518 байт UDP (Мбит/сек)[2]	76 000	**Application Control (МЭ+DPI)[3] (Мбит/сек)**	16 000 (ограничение средства измерения)	**SSL Inspection[5]**	*
МЭ (пакетов/сек)	6 600 000	**NGFW Throughput (Мбит/с)[4]**	13 500	**Кол-во одновременно обслуживаемых соединений**	30 000 000 (ограничение средства измерения)
МЭ, TCP (Мбит/сек)	36 000 (ограничение средства измерения)	**Соединений в секунду**	622 000		

Аппаратные характеристики

Форм-фактор	ПАК (19′ Rack 2U)	**Источник питания**	Два встроенных БП с функцией «горячей» замены, 110-240 В, 800 Вт	**Сетевые порты**	4 x RJ45 1 Гбит/с 4 x SFP 1 Гбит/с 8 x SFP+ 10Гбит/с
Размеры (ШхВхГ)	483 x 88 x 558 мм	**Порты ввода/вывода**	1 x VGA 2 x USB 3.0 (тип A) 1 x USB 3.0 (тип C) 1 x miniUSB (тип B)		
Масса	До 24 кг				

[1]Производительность исполнения зависит от аппаратной платформы, 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 SSL/TLS соединений, осуществляется методом измерения показателей передачи HTTPS-трафика. Измерение производительности проводится на фоне передачи вредоносного трафика, который должен отфильтровываться контентными фильтрами и антивирусной проверкой.

*Результаты будут предоставлены позже.

инфотекс

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

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

CH26_00RU

ViPNet Virtual Private Network