

## Варианты внедрения

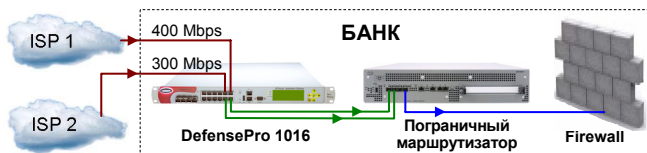
Решение для защиты от DDoS-атак **Radware DefensePro** компании **Radware** представлено тремя линейками:

- Radware DefensePro x016 IPS & Behavioral Protection
- Radware DefensePro x412 IPS & Behavioral Protection
- Radware DefensePro x412 Behavioral Protection

DefensePro включается в разрыв Ethernet-соединения, работает в режиме «in-line», невидим для сетевого оборудования (Transparent L2 Forwarding) и контролирует весь трафик с целью предотвращения DDoS-атак.

Если в банк приходит несколько Интернет-каналов с суммарной пропускной способностью более 500 Mbps и при этом банк имеет свою автономную систему (то есть IP-пакет может прийти в банк по одному каналу, а уйти – по другому), то DefensePro следует устанавливать в банке и включать в разрыв каждого Интернет-канала.

В такой схеме DefensePro сможет анализировать и сопоставлять весь входящий и весь исходящий трафик по всем Интернет-каналам одновременно, выявлять и предотвращать сканирования, проникновения «сетевых червей» и работу «ботов», уклоняться от DDoS-атак.



Если пропускная способность всех Интернет-каналов банка не превышает суммарно 100 Mbps, то установка в банке DefensePro не позволит эффективно бороться с DDoS-атаками. Интернет-каналы с низкой пропускной способностью могут быть перегружены примитивными сетевыми DDoS-атаками (TCP SYN, UDP и ICMP flood).

В таких случаях DefensePro необходимо устанавливать в дата-центре канального провайдера банка, подключать к провайдеру по 1Gb, транком из нескольких 1Gb или же по 10Gb и осуществлять на DefensePro очистку всего трафика до «узкого» банковского Интернет-канала.



## Технические подробности

DefensePro – это специализированная платформа с двумя процессорами Dual-Core Opteron, с 6..10 Гбайт оперативной памяти, со встроенными высокопроизводительными сетевыми процессорами компании EZChip Technologies, со специализированными ASIC и FPGA для аппаратного ускорения обработки сетевого трафика.

DefensePro со встроенным IPS содержит также высокопроизводительный контекстный процессор NETL7 компании NetLogic Microsystems для аппаратного ускорения сигнатурного анализа сетевых пакетов.



Обработка сетевого трафика осуществляется поэтапно с использованием различных механизмов защиты. При этом суммарное время задержки сетевого пакета для всех линеек DefensePro не превышает 60 микросекунд.

В DefensePro реализованы следующие механизмы защиты:

- Behavioral DDoS Protection
- TCP SYN Flood Protection
- Signature Protection (IPS)
- Connection Limit
- Stateful Inspection
- BandWidth Management
- HTTP Mitigator
- Behavioral Server-Cracking Protection
- Anti-Scanning Protection
- Stateful Firewall (ACL)

Одно из достоинств DefensePro – это возможность увеличения производительности по мере необходимости.

На начальном этапе банк приобретает DefensePro 1016 с производительностью 1Gbps при минимальном бюджете. В дальнейшем при росте нагрузки банк может увеличить производительность DefensePro до 2Gbps или 3Gbps простой докупкой лицензии.

Ниже представлена таблица с ценами и техническими характеристиками всех моделей Radware DefensePro.

Характеристики	DefensePro x016 IPS & Behavioral Protection			DefensePro x412 IPS & Behavioral Protection		DefensePro x412 Behavioral Protection		
	1016	2016	3016	4412	8412	4412	8412	12412
Цена* с НДС, USD (ЦБ + 3%)	49'500	77'000	99'000	132'000	187'000	99'000	143'000	187'000
Платформа	OnDemand Switch 2S1			OnDemand Switch 3S2		OnDemand Switch 3S1		
Производительность	1 Gbps	2 Gbps	3 Gbps	4 Gbps	8 Gbps	4 Gbps	8 Gbps	13 Gbps
Макс. кол-во конкурентных сессий	2'000'000			3'200'000		4'000'000		
Макс. кол-во пакетов в секунду	1'000'000 pps			10'000'000 pps				
Порты для инспекции трафика	4*1Gb SFP + 12*1Gb UTP			4*10Gb XFP + 4*1Gb SFP + 8*1Gb UTP				

\* Для всех трех линеек Radware DefensePro существуют ежегодные затраты на техническую поддержку (один из пяти уровней). Для двух линеек со встроенным IPS – DefensePro x016 IPS & Behavioral Protection и DefensePro x412 IPS & Behavioral Protection – есть также дополнительные ежегодные затраты на Security Update Service (сервис обновления сигнатур IPS) – см. далее.

## О механизмах защиты

**Behavioral DDoS Protection.** Самый действенный и самый ресурсоемкий механизм защиты от DDoS-атак.

В основе поведенческой защиты – глубокая инспекция пакетов вплоть до 7-го уровня (Deep Packet Inspection), накопление и анализ статистики, обучение и адаптивное построение многомерной модели распределения трафика для штатных условий работы защищаемых сетей и сетевых сервисов, выявление DDoS-атак на основе отклонений и аномалий, блокирование нелегитимного трафика методом динамической фильтрации сетевых пакетов с автоматической генерацией сигнатур DDoS-атаки в реальном времени (модуль Fuzzy Logic).



Механизм поведенческой защиты имеет большое количество настраиваемых параметров, поддерживает периоды обучения длительностью день, неделя и месяц, позволяет создавать отдельные политики для каждой защищаемой сети и для каждого сетевого сервиса.

При обнаружении признаков DDoS-атаки время на принятие решения, построение динамических фильтров и генерацию сигнатур DDoS-атаки составляет 12 секунд.

В процессе подавления DDoS-атаки механизм поведенческой защиты отслеживает количественные и качественные параметры трафика и при снижении сетевой активности ниже критических порогов снимает динамические фильтры и деактивирует сигнатуры.

Если же применение построенных динамических фильтров и сгенерированных сигнатур не привело к снижению нелегитимного трафика ниже пороговых значений, то DefensePro осуществляет анализ дополнительных параметров трафика с последующим ужесточением фильтрации и регенерацией сигнатур.

Одно из важных преимуществ механизма поведенческой защиты DefensePro – противодействие атакам «нулевой минуты», для которых еще не созданы статические сигнатуры и не может быть применен IPS.

**TCP SYN Flood Protection.** Высокопроизводительный (до 10 Mpps) механизм защиты от атак TCP SYN flood с подменой IP-адреса отправителя (спуфинг). В основе – механизм SYN Cookies, поддерживаемый встроенными в DefensePro сетевыми процессорами EZChip и FPGA.

**Signature Protection.** Классический IPS с аппаратной поддержкой статических сигнатур, разработанных и постоянно обновляемых компанией Radware, а также сигнатур пользователя. Присутствует только в двух линейках DefensePro.

Высокопроизводительный аппаратный IPS является оптимальным методом противодействия известным уязвимостям в ПО и DDoS-атакам, реализуемым на базе широко распространенных утилит и конструкторов.

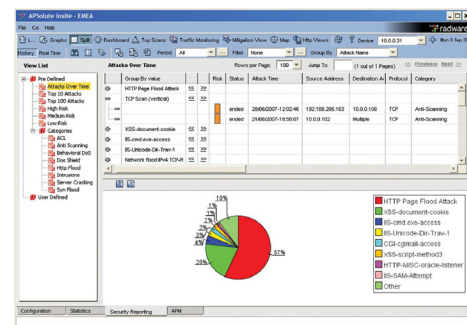
Использование DefensePro со встроенным IPS позволит банку исключить риски проникновения «сетевых червей», детектировать работу «ботов» на компьютерах банковских сотрудников, защитить сетевые сервисы от атак на выявленные, но еще не закрытые уязвимости в серверном ПО, противодействовать типовым DDoS-атакам.

**Connection Limit.** Данный механизм для защищаемого сервиса обеспечивает контроль максимально допустимого количества сессий с IP-адреса отправителя в единицу времени и при превышении пороговых значений блокирует трафик с чрезмерно активных хостов.

**Stateful Inspection.** Данный механизм проверяет протоколы TCP, ICMP, DNS, HTTPS, SMTP, IMAP, POP3, FTP и SSH на полное соответствие спецификациям RFC. Механизм предотвращает атаки, основанные на нарушении последовательностей пакетов указанных протоколов.

**BandWidth Management.** Данный механизм позволяет банку для заданного протокола, защищаемой сети или сетевого сервиса выделить минимально гарантированную полосу пропускания и, при необходимости, ограничить полосу максимально допустимым значением.

DefensePro содержит гибкие механизмы онлайн-мониторинга трафика, оперативного информирования об инцидентах, построения развернутых отчетов.



Компания «БИФИТ» является официальным сертифицированным партнером компании Radware и предоставляет в **опытную эксплуатацию** решения Radware DefensePro.

За информацией о решениях Radware DefensePro обращайтесь по тел. +7 (495) 797-88-89 и e-mail: [antiddos@bifit.com](mailto:antiddos@bifit.com)

Ниже представлена таблица с ценами на сервис обновления сигнатур IPS и техническую поддержку для всех моделей Radware DefensePro (курс ЦБ РФ + 3%).

Цены с НДС на сервис обновления сигнатур IPS и на техническую поддержку, USD	DefensePro x016 IPS & Behavioral Protection			DefensePro x412 IPS & Behavioral Protection		DefensePro x412 Behavioral Protection		
	1016	2016	3016	4412	8412	4412	8412	12412
Security Update Service, USD в год	3'713	5'775	7'425	9'900	14'025	-		
Support Certainty Level 1, USD в год	5'940	9'240	11'880	15'840	22'440	11'880	17'160	22'440
Support Certainty Level 2, USD в год	7'920	12'320	15'840	21'120	29'920	15'840	22'880	29'920
Support Certainty Level 3, USD в год	8'910	13'860	17'820	23'760	33'660	17'820	25'740	33'660
Support Certainty Level 4, USD в год	10'395	16'170	20'790	27'720	39'270	20'790	30'030	39'270
Support Certainty Level 5, USD в год	12'375	19'250	24'750	33'000	46'750	24'750	35'750	46'750