



Check Point DDoS Protector™

Остановите атаки Отказа в обслуживании за секунды при помощи настраиваемой, многоуровневой защиты, которая блокирует широкий спектр атак.

Устройство Check Point DDoS Protector

Из всего спектра современных угроз, атаки «Отказ в обслуживании (DoS)» возрастают в количестве, скорости и сложности. Атаки Отказ в обслуживании и Распределенный отказ в обслуживании (DDoS) относительно легко выполнимы, и могут нанести серьезный ущерб компаниям, работа которых зависит от web-сервисов. Многочисленные (более 50) «инструментарии» для DDoS-атаки без труда доступны в Интернете, и все большее число атак инициированы в более чем 230 странах. DDoS-атаки часто используются для извлечения прибыли: в 2011 году, кибер-преступники заработали колоссальные \$ 12,5 миллиарда долларов. 2012 показывает тревожную волну DDoS угроз в сфере финансовых услуг. Однако «хактивизм» и политические мотивы быстро становятся самым популярным форумом для запуска атак отказа в обслуживании. Группы Anonymous успешно возглавляла многочисленные кампании атак на отдельных лиц, организации, правительства и страны в отместку за действия или заявления, с которыми они не согласны.

Многие DDoS-решения разворачиваются Интернет-провайдерами, предлагая типовую защиту от атак на сетевом уровне. Однако современные DDoS-атаки становятся все более изощренными, направляя многочисленные атаки на сети и приложения. Успешные DDoS-решения должны предлагать компаниям возможность настроить собственную защиту для удовлетворения меняющихся требований в области безопасности, быстрое время отклика во время атаки, и выбор вариантов развертывания.

ОБЗОР

Новое Устройство Check Point DDoS Protector поддерживает работоспособность компании при помощи многослойной, настраиваемой защиты и производительности 12Гбит/с. Устройство автоматически защищает от сетевого флуда и атак на прикладном уровне, обеспечивая высокое быстродействие против современных изощренных атак отказа в обслуживании. Устройства DDoS Protector предлагают гибкие варианты развертывания для легкой защиты компании любого размера, встроенного управления безопасностью для исследования трафика в режиме реального времени и анализа угроз для продвинутой защиты от DDoS-атак. Check Point также предлагает специализированную поддержку в режиме 24/7 и ресурсы для обеспечения самой современной защиты.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- Защита от известных и неизвестных DDoS-атак
- Защищает от атак на сетевом и на прикладном уровне
- Гибкие фильтрующие движки обнаруживают и предотвращают вредоносные эксплойты
- Защищает от атак на HTTP
- Защищает от атак флуда, направленных на уменьшение пропускной способности
- Быстрое, гибкое создание сигнатур поддерживает работоспособность компаний

ПРЕИМУЩЕСТВА

- Защита от разрастания атак DDoS, минимизирующая последствия для бизнеса
- Передовые технологии помогают поддерживать web-сервисы в рабочем состоянии во время нападения
- Полностью готовое к работе устройство прямо из коробки
- Интегрированное с системой управления безопасностью Check Point для большей наглядности и контроля
- Высокоэффективное DDoS-решение с производительностью 14Гбит/с и пропускной способностью 12Гбит/с
- Многоуровневая защита блокирует различные типы атак
- Настраиваемая защита подходит под любые требования к безопасности и для компании любого размера
- Гибкие варианты развертывания включают установку на месте или у вашего Интернет-провайдера



МНОГОУРОВНЕВАЯ ЗАЩИТА

Защита сети и защита от атак флуда

Защита от DDoS-атак, направленных на сети, используя:

Поведенческие атаки DoS – защита от TCP, UDP, ICMP, IGMP и фрагментированных DDoS-атак с адаптивным обнаружением на поведенческой основе.

DoS экран – защита от известных инструментов DDoS-атак при помощи заранее определенных и настроенных фильтров для ограничения скорости по шаблону.

Суп-защита – блокирует DoS-атаку имитации SYN с использованием порога скорости SYN-пакетов для каждого защищаемого сервера.

Черный список – блокирует типовые атаки при помощи классификации источник-приемник на уровнях L3 и L4 и правил истечения срока действия.

Ограничение скорости соединения – блокирует типовые, не поддерживаемые протоколы (не DNS, HTTP) и флуд-атаки прикладного уровня, скорость которых выше пороговых значений.

DoS/DDoS-защита на уровне приложений

Защищает от более сложных DDoS-атак, которые злоупотребляют ресурсами приложений с помощью:

SYN-защита с web-вызовом – защищает от DoS-атак основанных на соединении HTTP с использованием порога скорости SYN-пакетов для каждого защищаемого сервера.

Поведенческая защита DNS – блокирование DNS запросов DoS-атак с адаптивным обнаружением на основе поведения DNS, используя определяемые пороговые скорости блокировки DNS, а также вызовов и реакцию DNS.

Поведенческая защита HTTP («подавление HTTP») – блокирует как DoS-атаки использующие HTTP-соединение, так и атаки на пропускную способность HTTP в восходящем направлении, с помощью адаптивного поведенческого обнаружения на базе сервера, определения работы HTTP с вызовами и реакциями web, сообщением 302 redirect, а также вызовами JS.

Приложение, ориентированное на защиту от DoS/DDoS

Отражает DoS и DDoS-атаки, которые требуют особых критериев фильтрации. Гибкое определение фильтрации осуществляет поиск по шаблону конкретного содержимого в каждом пакете. Включает способность анализировать и блокировать продолжающиеся атаки путем определения защиты на лету.

УПРАВЛЕНИЕ

Устройства DDoS интегрированы с Управлением Безопасностью Check Point, включая:

SmartEvent

Решение, объединяющее события безопасности и анализ, которое обеспечивает в режиме реального времени информацией по управлению угрозами, чтобы мгновенно остановить угрозы и блокировать атаки с защитой на лету. Переход от осмотра работы к экспертизе всего за три щелчка.

SmartLog

Расширенный анализатор журналов, который обеспечивает интеллектуальную проактивную защиту с мгновенными результатами поиска из любого поля журнала для текущей наглядности миллиардов записей журнала в течение нескольких периодов времени и многочисленных доменов.

SmartView Tracker

Решение всестороннего аудита для поиска и устранения неисправностей в системе и вопросов безопасности, сбор информации для правовой оценки и в целях аудита, генерация отчетов для анализа графиков сетевого трафика. В случае атаки или другой подозрительной сетевой активности, используется SmartView Tracker, чтобы временно или навсегда прекратить соединения с определенных IP-адресов.

Оповещение

SNMP V1, 2C и 3, журнал регистрации, Syslog, электронная почта

Конфигурация

SNMP, V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, SOAP API, Console (по выбору пользователя).

Синхронизация времени

На основе сетевого протокола NTP.

Экспорт информации о сигнатуре в режиме реального времени

Передовой XML интерфейс экспортирует поведенческие параметры.



Check Point DDoS Protector
**ТЕХНИЧЕСКИЕ
ХАРАКТЕРИСТИКИ**


Модель DDoS Protector	506	1006	2006	3006	4412	8412	12412
Класс сети	Корпоративная				Центр обработки данных		
Быстродействие¹							
Производительность ²	500Mbps	1Gbps	2Gbps	3Gbps	4Gbps	8Gbps	14Gbps
Пропускная способность ³	500Mbps	1Gbps	2Gbps	3Gbps	4Gbps	8Gbps	12Gbps
Максимальное число одновременных сессий	2,000,000	2,000,000	2,000,000	2,000,000	4,000,000	4,000,000	4,000,000
Максимальный уровень предотвращения DDoS флуд-атак (пакетов в секунду)	1,000,000	1,000,000	1,000,000	1,000,000	10,000,000	10,000,000	10,000,000
Задержка	< 60 микро секунд						
Сигнатуры в режиме реального времени	Обнаружение и защита от атак менее чем за 18 секунд						
Количество контролируемых портов							
10/100/1000 Ethernet (медный кабель)	4	4	4	4	8	8	8
GbE (SFP)	2	2	2	2	4	4	4
10GbE (XFP)	-	-	-	-	4	4	4
Количество портов управления							
10/100/1000 Ethernet (медный кабель)	2	2	2	2	2	2	2
RS-232	1	1	1	1	1	1	1
Режим работы							
Работа в сети	Прозрачная переадресация на уровне L2						
Способы развертывания	in-line; мониторинг диапазона портов; копия с порта захвата; локальное ответвление; подавление ответвления						
Поддерживаемые протоколы туннелирования	VLAN Tagging, L2TP, MPLS, GRE, GTP						
IPv6	Поддержка сетей IPv6 и блокирование атак на сети IPv6						
Действия политики	Блокировать и Отчет; Только отчет						
Блокирующие действия	Сбросить пакет, сбросить (источник, место назначения, и то и другое), приостановить (источник, порт источника, место назначения, порт места назначения или любая комбинация); запрос-ответ для HTTP и DNS атак						
Высокая готовность (High Availability)							
Fail-open / Fail-close	Внутренний модуль fail-open/fail-close для портов (медный кабель); внутренний модуль fail-close для SFP портов; опционально fail-open для SFP портов ⁴				Внутренний модуль fail-open/fail-close для портов (медный кабель); внутренний модуль fail-close для SFP и XFP портов; опционально fail-open для SFP и XFP портов ⁵		
SKU	CPAP-DP506	CPAP-DP1006	CPAP-DP2006	CPAP-DP3006	CPAP-DP4412	CPAP-DP8412	CPAP-DP12412

¹ Фактические показатели быстродействия могут изменяться в зависимости от конфигурации сети, типа трафика и т.д.

² Производительность измеряется как максимальное значение переадресации трафика при отсутствии настроенного профиля безопасности

³ Пропускная способность измеряется с поведенческой защитой и защитой сигнатур с использованием профиля защиты eCommerce

⁴ Внешний волоконно-оптический fail-open коммутатор с SFP портами доступен за дополнительную плату

⁵ Внешние волоконно-оптические fail-open коммутаторы с SFP или XFP портами доступны за дополнительную плату



Аксессуары для DDoS Protector	SKU
Съемный 10Гбит/с оптический (XFP) одномодовый LR-адаптер	CPAC-DP-10LR-XFP
Съемный 10Гбит/с оптический (XFP) многомодовый SR-адаптер	CPAC-DP-10SR-XFP
Съемный 1Гбит/с оптический одномодовый ZX-адаптер	CPAC-DP-1ZX-SFP
Съемный 1Гбит/с 1000BASE-T адаптер (витая пара)	CPAC-DP-1C-SFP
Съемный 1Гбит/с оптический одномодовый LX-адаптер	CPAC-DP-1LX-SFP
Съемный 1Гбит/с оптический многомодовый SX-адаптер	CPAC-DP-1SX-SFP
10Гбит/с внешний модуль обхода, поддерживающий один LR сегмент – защищает от сбоя питания и сбоя соединения, для DDoS Protector серии x412	CPAC-DP-1LR-10BP
10Гбит/с внешний блок обхода, включает один LR сегмент, расширяется до четырех сегментов – защищает от сбоя питания и сбоя соединения, для DDoS Protector серии x412	CPAC-DP-4LR-10BP
10Гбит/с внешний модуль обхода, сегмент интерфейса LR – защищает от сбоя питания и сбоя соединения, для DDoS Protector серии x412	CPAC-DP-1LR-10BPM
10GbE External Bypass chassis, includes one SR interface segment, expandable up to four (4) segments - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-4SR-10BP
10Гбит/с внешний модуль обхода, сегмент интерфейса SR – защищает от сбоя питания и сбоя соединения, для DDoS Protector серии x412	CPAC-DP-1SR-10BPM
1Гбит/с внешний модуль обхода, поддерживающий один SX сегмент – защищает от сбоя питания и сбоя соединения, для DDoS Protector серии x412	CPAC-DP-1SX-1BP
1Гбит/с внешний модуль обхода, поддерживающий один LX для SX сегмента – защищает от сбоя питания и сбоя соединения, для DDoS Protector серии x412	CPAC-DP-1LX-1BP
Занимает 2RU в стойке для коммутаторов обхода	CPAC-DP-2RM
Двойной источник питания постоянного тока для DDoS Protector серии x412	CPAC-DP-2PS-DC
Один источник питания постоянного тока для DDoS Protector серии x412	CPAC-DP-PS-DC