Check Point
SOFTWARE TECHNOLOGIES LTD.

УСТРОЙСТВА CHECK POINT

2018

СОДЕРЖАНИЕ

УСТРОЙСТВА CHECK POINT

03 ЗАЩИТА ОТ УГРОЗ НОВОГО ПОКОЛЕНИЯ

04 ЗАЩИЩЕННАЯ ОС, СДЕЛАННАЯ ДЛЯ ВАС

05 АППАРАТНЫЕ ШЛЮЗЫ БЕЗОПАСНОСТИ

13 ВИРТУАЛЬНЫЕ ШЛЮЗЫ БЕЗОПАСНОСТИ

14 УСТРОЙСТВА SMART-1

15 УСТРОЙСТВА ЗАЩИТЫ ОТ DDoS

16 УСТРОЙСТВА SANDBLAST

17 ПРОВЕРЕННОЕ КАЧЕСТВО ЗАЩИТЫ

ЗАЩИТА ОТ УГРОЗ НОВОГО ПОКОЛЕНИЯ

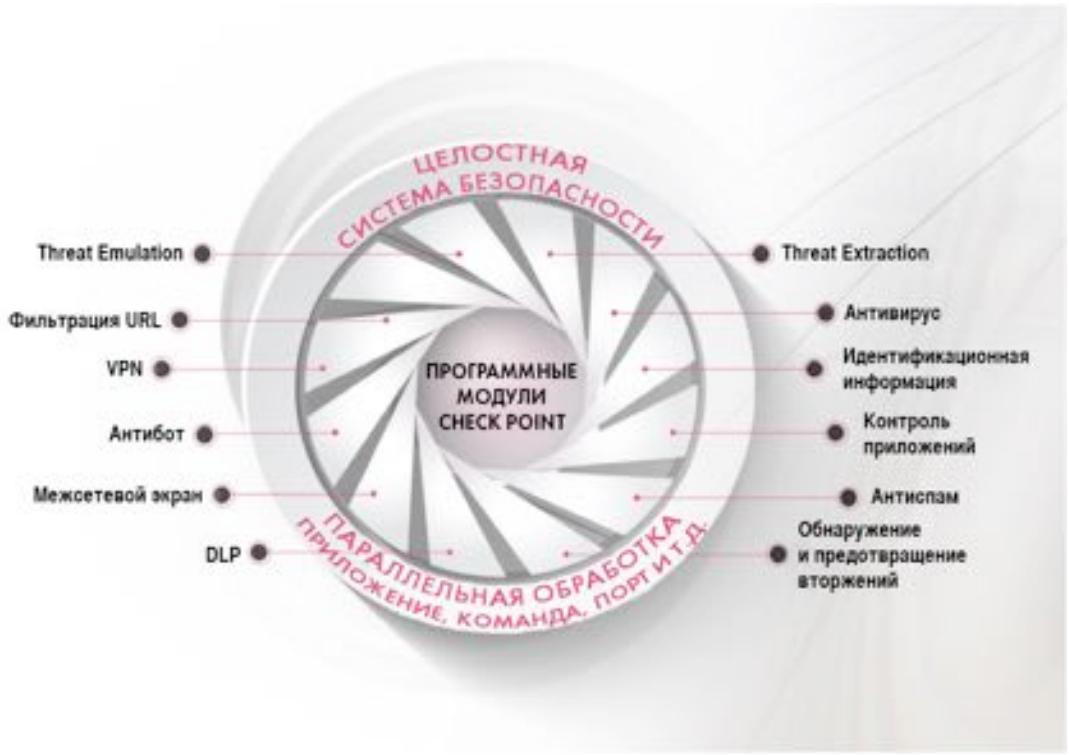
КОМПЛЕКСНОЕ ПРЕДОТВРАЩЕНИЕ УГРОЗ

Быстрый рост вредоносного ПО, растущее мастерство хакеров и появление новых неизвестных угроз «нулевого дня» требуют применение иного подхода к защите корпоративных сетей и данных. Check Point обеспечивает полностью интегрированную комплексную защиту для борьбы с этими возникающими угрозами, одновременно уменьшая сложность и повышая эффективность работы. Решение Check Point Threat Prevention включает в себя мощные функции безопасности, такие как межсетевой экран, систему предотвращения вторжений (IPS), антибот, антивирус, управление приложениями и фильтрацию URL-адресов для борьбы с известными кибератаками и угрозами – улучшенную теперь отмеченными наградами системами SandBlast™ Threat Emulation и Threat Extraction для полной защиты от наиболее сложных угроз и уязвимостей «нулевого дня».

ПРЕДОТВРАЩАЯ ИЗВЕСТНЫЕ УГРОЗЫ И УГРОЗЫ «НУЛЕВОГО ДНЯ»

В рамках решения Check Point SandBlast Zero-Day Protection облачный механизм Threat Emulation обнаруживает вредоносное ПО на этапе эксплойта даже до того, как хакеры смогут применить методы уклонения, пытаясь обойти «песочницу». Файлы помещаются в карантин и проверяются путем запуска в виртуальной «песочнице», чтобы обнаружить вредоносное поведение, прежде чем они попадут в вашу сеть. Это инновационное решение сочетает в себе проверку логики исполнения программы на уровне центрального процессора и динамический анализ в песочнице сразу в нескольких ОС для предотвращения самых опасных эксплойтов, атак «нулевого дня» и таргетированных атак.

Динамический анализ файлов может занимать минуты. Технология SandBlast Threat Extraction удаляет потенциально опасное содержимое документов и изображений, включая активный контент и встроенные объекты, реконструирует файлы для устранения потенциальных угроз и мгновенно доставляет очищенный 100% безопасный контент пользователям, обеспечивая эффективность бизнес-процесса.



ЗАЩИЩЕННАЯ ОС НОВОГО ПОКОЛЕНИЯ, СДЕЛАННАЯ ДЛЯ ВАС

GAIA – УНИФИЦИРОВАННАЯ ЗАЩИЩЕННАЯ ОПЕРАЦИОННАЯ СИСТЕМА

Check Point GAiA™ – это защищенная операционная система нового поколения для всех устройств Check Point, серверов открытой архитектуры и виртуализированных шлюзов. Клиенты получают выгоду от высокоэффективной 64-битной ОС, увеличенной емкости подключения устройств и упрощенных процессов эксплуатации. GAiA упрощает управление с разделением обязанностей между пользователями с разными привилегиями, предоставляя управление на основе ролей. Возможности автоматического обновления программного обеспечения повышают эффективность работы, а интуитивно понятный и многофункциональный веб-интерфейс позволяет выполнять поиск любой команды или настройки за секунду. Сети IPv4 и IPv6 защищаются с применением технологий ускорения и кластеризации и поддерживают самые последние юникастные и мультикастные протоколы маршрутизации.

ВИРТУАЛИЗАЦИЯ ШЛЮЗОВ БЕЗОПАСНОСТИ

Виртуальные системы Check Point позволяют организациям консолидировать инфраструктуру за счет создания нескольких виртуализированных шлюзов безопасности на одном аппаратном устройстве, что обеспечивает значительную экономию средств благодаря бесшовной консолидации безопасности и инфраструктуры. Оптимизированное управление виртуализованными шлюзами дополнительно повышает операционную эффективность IT-отдела с ограниченными ресурсами, обеспечивая необходимую простоту сетевой безопасности.

НОВЫЙ СПОСОБ ИЗМЕРЕНИЯ РЕАЛЬНОЙ МОЩНОСТИ УСТРОЙСТВ БЕЗОПАСНОСТИ

В отличие от других компаний, которые указывают показатели производительности в идеальных лабораторных условиях тестирования на больших пакетах и используют политику безопасности, которая имеет только одно правило Accept Any, производительность устройства безопасности Check Point измерена на реалистичном смешанном трафике клиентов, с применением рекомендуемого набора функций глубокой инспекции трафика и защиты от угроз и типичной политики безопасности. SecurityPower™ обеспечивает эффективный показатель для выбора правильного устройства, которое лучше прогнозирует его текущее и будущее поведение при атаках на безопасность и в повседневной работе. Клиентам гарантируется, что они получают устройство безопасности, отвечающее их текущим потребностям и обеспечивающее возможности для роста.

SecurityPower

АППАРАТНЫЕ ШЛЮЗЫ БЕЗОПАСНОСТИ

Check Point предоставляет компаниям любых размеров новейшие решения по защите данных и сетевой безопасности на интегрированных платформах предотвращения угроз следующего поколения, снижая сложность и снижая общую стоимость владения. Если вам нужна безопасность следующего поколения для вашего центра обработки данных, предприятия, малого бизнеса или домашнего офиса, у Check Point есть решение для вас.

 Филиал	Использование	Филиальный или малый офис	1400
	Форм-фактор	Настольный	3100, 3200
	Интерфейсы	1 GbE, 802.11n/ac Wi-FI, 3G/4G, PoE	5100
	Производительность МСЭ	От 750 Мбит/с до 14.5 Гбит/с	
	Специфические особенности	Веб-управление	
 Предприятие	Использование	Предприятие	5200
	Форм-фактор	1RU	5400, 5600
	Интерфейсы	1, 10, 40 GbE	5800, 5900
	Производительность МСЭ	От 3 до 52 Гбит/с	
	Специфические особенности	Гибкость вариантов ввода-вывода, LOM	
 Центр обработки данных	Использование	Большое предприятие, ЦОД	15400, 15600 23500, 23800
	Форм-фактор	2RU	
	Интерфейсы	1, 10, 25, 40, 100 GbE	
	Производительность МСЭ	От 25 до 128 Гбит/с	
	Специфические особенности	25/40/100 GbE, питание от постоянного тока, LOM	
 Модульные шасси	Использование	ЦОД, Телко, Провайдеры	44000
	Форм-фактор	От 6RU до 16RU	64000
	Интерфейсы	1, 10, 40, 100 GbE	
	Производительность МСЭ	От 80 до 880 Гбит/с	
	Специфические особенности	Модульная, масштабируемая платформа	
 Защищенное исполнение	Использование	Агрессивные среды	1200R
	Форм-фактор	Desktop, DIN mount	
	Интерфейсы	1 GbE, поддержка 3G/4G	
	Производительность МСЭ	2 Гбит/с	
	Специфические особенности	Питание от постоянного/переменного тока	

УСТРОЙСТВА 1400

БЕЗОПАСНОСТЬ ФИЛИАЛЬНЫХ ОФИСОВ

1430-1450
(ВАРИАНТ С WI-FI)

1470-1490
(ВАРИАНТ С WI-FI)

ОБЗОР

Обеспечение надежной сетевой безопасности на предприятии является сложной задачей, когда граница предприятия распространяется на удаленные и филиальные офисы, где есть несколько пользователей, которые имеют малый опыт работы с IT. Удаленные офисы и филиалы требуют такого же уровня защиты от сложных кибератак и угроз «нулевого дня», как и главные корпоративные офисы. Устройства Check Point 1400 - это доступное и простое решение «все-в-одном» для обеспечения лучшей в отрасли безопасности для защиты самого слабого звена в вашей корпоративной сети - удаленных филиалов.

Теперь вы можете защитить всю свою сеть – от штаб-квартиры до удаленных офисов – от киберугроз с помощью передовой технологии предотвращения угроз Check Point Threat Prevention. Устройства 1400 идеально подходят для небольших офисов. Для местного управления и поддержки в небольшой офисной среде доступен простой и интуитивно понятный веб-интерфейс управления через Интернет. Предприятия, которые хотят управлять безопасностью из центрального офиса, могут использовать средства управления безопасностью Check Point Security Management или мультидоменную систему Multi-Domain Security Management для удаленного управления и единообразного применения политики безопасности для сотен устройств на местах.

ВСЕОБЪЕМЛЮЩАЯ БЕЗОПАСНОСТЬ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Имеются разнообразные варианты сетевых интерфейсов, в том числе Ethernet-порты 1GbE, PoE, WiFi 802.11b/g/n/ac с гостевым доступом, беспроводные соединения 3G и 4G.

Максимальные показатели	1430	1450	1470	1490
Производительность МСЭ[1]	900 Мбит/с	1.1 Гбит/с	1.6 Гбит/с	1.8 Гбит/с
Производительность предотвращения угроз[1]	90 Мбит/с	150 Мбит/с	175 Мбит/с	220 Мбит/с
Порты 1 GbE	1x WAN, 1x DMZ, 6x коммутатор LAN		1x WAN, 1x DMZ, 16x коммутатор LAN	
Вариант Wi-Fi	802.11 b/g/n/ac, один диапазон 2.4 или 5GHz		802.11 b/g/n/ac, двойной диапазон 2.4 и 5GHz	
Наличие PoE	✗		✓	

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/branch-office-security/

ИНДУСТРИАЛЬНОЕ УСТРОЙСТВО 1200R

БЕЗОПАСНОСТЬ ДЛЯ АГРЕССИВНЫХ СРЕД

1200R

ОБЗОР

Защита критической инфраструктуры от кибератак создает уникальные проблемы. Среда может быть агрессивной, а системы часто используют специализированные протоколы. Решения Check Point для кибербезопасности АСУ ТП обеспечивают расширенную защиту от угроз в сочетании с вариантами защищенных индустриальных устройств и всесторонней поддержкой протоколов, чтобы гарантировать, что жизненно важные активы, такие как объекты производства электроэнергии, системы управления движением, системы очистки воды и заводы, никогда не будут скомпрометированы.

Устройство 1200R дополняет наше обширное семейство устройств для поддержки разнообразных сред развертывания и удовлетворения особых требований. Например, 1200R соответствует промышленным спецификациям, таким как IEEE 1613 и IEC 61850-3 по нагреву, вибрации и защите от электромагнитных помех (EMI). При экстремальных температурах от -40°C до +75°C, когда другие устройства не работают, это устройство защищает вас.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Имеются медные и оптоволоконные порты Ethernet 1GbE, а также поддержка беспроводного соединения 3G и 4G через совместимые USB-модемы.

Максимальные показатели	1200R
Производительность МСЭ (Мбит/с) [1]	700
Производительность IPS (Мбит/с) [1]	60
WAN	1x 10/100/1000BaseT RJ45 или 1x 1000BaseF порт
DMZ	1x 10/100/1000BaseT RJ45 или 1x 1000BaseF порт
LAN	Порты 4x 10/100/1000BaseT RJ45
Варианты установки	Рейка DIN или монтажная стойка
Промышленные сертификации	IEEE 1613, IEC 61850-3
Питание	Постоянный или переменный ток

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/industrial-control-systems-appliances

УСТРОЙСТВА 3000

БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ ДЛЯ ФИЛИАЛЬНЫХ ОФИСОВ

3100

3200

ОБЗОР

Целостная безопасность требует последовательной защиты повсеместно, а не только в основной корпоративной сети. Равный уровень защиты необходим и для удаленных офисов и филиалов, чтобы сформировать единую и полную защиту от потенциальных угроз. Устройства Check Point 3000 представляют собой идеальное решение для обеспечения безопасности в небольших офисах и филиалах.

Устройства 3000 предлагают безопасность корпоративного уровня без компромиссов в компактном настольном форм-факторе. Многоядерные технологии, шесть портов 1 Gigabit Ethernet и расширенные возможности предотвращения угроз легко расширяют надежную защиту для удаленных филиалов и небольших офисов. Несмотря на малый форм-фактор, эти мощные устройства обеспечивают до 2,1 Гбит/с реальной пропускной способности в режиме межсетевого экрана и до 160 Мбит/с реальной пропускной способности в режиме предотвращения угроз.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™ ZERO-DAY PROTECTION

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Компактная конструкция, многоядерные технологии и защита от угроз «нулевого дня» SandBlast, доступные в устройствах 3000, делают эти шлюзы идеально подходящими для развертывания в небольших офисах и удаленных филиалах.

Максимальные показатели	3100	3200
Производительность МСЭ (Гбит/с) [1]	2.1	2.1
Производительность NGFW (МСЭ, Контроль приложений, IPS) (Мбит/с) [1]	220	260
Производительность предотвращения угроз (Мбит/с) [1]	130	160
Порты 1 GbE (медь)	6	
ОЗУ	8 ГБ	
Система хранения	1x 320ГБ (HDD) или 1x 240ГБ (SSD)	
Корпус	Настольный	

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/branch-office-security/

УСТРОЙСТВА 5000

БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ, ГИБКИЕ СЕТЕВЫЕ ОПЦИИ

5100 5200 5400 5600 5800 5900

ОБЗОР

Решения безопасности больше не должны быть выбором между функционалом и производительностью. Специально разработанные устройства Check Point 5000 без компромиссов обеспечивают самую передовую защиту от угроз для требовательных сетей среднего и малого бизнеса.

Устройства Check Point 5000 сочетают в себе возможности нескольких сетевых интерфейсов с возможностями высокопроизводительных многоядерных систем, обеспечивая исключительную многоуровневую защиту без ущерба для производительности. В устройствах 5000 в компактный форм-фактор, монтируемый в стойку 1U, упакованы до максимум 16(26) портов 1 Gigabit Ethernet, резервные источники питания с возможностью «горячей» замены и дополнительный модуль внеполосного управления LOM. Поддерживая до 26 Гбит/с реальной пропускной способности МСЭ и 1,65 Гбит/с реальной пропускной способности в режиме предотвращения угроз, эти устройства обеспечивают лучшую производительность в своем классе.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast ZERO-DAY PROTECTION

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Модульная конструкция и широкий спектр сетевых опций, доступных в устройствах серии 5000, не только обеспечивают богатый набор возможностей подключения для этих шлюзов, но также делают эти шлюзы максимально настраиваемыми для размещения в любой сетевой среде.

Максимальные показатели	5100	5200	5400	5600	5800	5900
Производительность МСЭ (Гбит/с) [1]	4.2	5.3	10	17.5	22	26
Производительность предотвращения угроз (Гбит/с) [1]	250 Мбит/с	290 Мбит/с	395 Мбит/с	645 Мбит/с	1.035	1.65
Порты 1 GbE (медь)	14	14	18	18	26	26
Порты 1 GbE (оптоволокно)	4	4	4	4	8	8
Порты 10 GbE (оптоволокно)				4	8	8
ОЗУ	16 ГБ	16 ГБ	32 ГБ	32 ГБ	32 ГБ	32 ГБ
Система хранения	1x 500ГБ (HDD) или 1x 240ГБ (SSD)					2x диска
Источники питания переменного или постоянного тока	1	1	1	2	2	2
Внеполосное управление LOM	✓	✓	✓	✓	✓	✓
Слоты сетевых расширений	1	1	1	1	2	2

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/small-midsize-enterprise-security/

УСТРОЙСТВА 15000

ПРЕДОТВРАЩЕНИЕ УГРОЗ ДЛЯ БОЛЬШИХ ПРЕДПРИЯТИЙ

15400

15600

ОБЗОР

Крупные предприятия нуждаются в высокой производительности, работоспособности и масштабируемости. Устройства 15000 сочетают в себе самые надежные средства защиты со специально разработанным оборудованием. Эти мощные устройства безопасности оптимизированы для обеспечения пропускной способности в режиме предотвращения угроз на реальном трафике до 3 Гбит/с для обеспечения защиты наиболее важных активов.

Устройства Check Point 15000 идеально подходят для крупных корпоративных сетей, которые требуют высокой производительности и гибкости параметров ввода-вывода. Если вы готовы перейти от 10 на 25, 40 или 100 GbE, то готовы и устройства 15000. Это 2U-устройства с тремя слотами расширения ввода-вывода для обеспечения высокой плотности портов, с резервными источниками питания переменного или постоянного тока, с дисковым массивом RAID1 2x 1ТБ (HDD) или 2x 480ГБ (SSD) и портом LOM для удаленного внеполосного управления.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™ ZERO-DAY PROTECTION

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Модульная конструкция и широкий спектр сетевых опций, доступных в устройствах серии 15000, не только обеспечивают богатый набор возможностей подключения для этих шлюзов, но и делают их легко настраиваемыми для развертывания в любой сетевой среде.

Максимальные показатели	15400	15600
Производительность МСЭ (Гбит/с) [1]	30	30
Производительность предотвращения угроз (Гбит/с) [1]	1.695	3
Порты 1 GbE (медь)	26	26
Порты 10 GbE (оптоволокно)	12	12
Порты 40 GbE (оптоволокно)	4	4
Порты 100/25 GbE (оптоволокно)	4	4
ОЗУ	64 ГБ	64 ГБ
Система хранения	2x 1ТБ (HDD) или 2x 480ГБ (SSD)	
Источники питания переменного или постоянного тока	2	2
Внеполосное управление LOM	✓	✓
Виртуальные системы	40	80

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/large-enterprise-security/

УСТРОЙСТВА 23000

ПРЕДОТВРАЩЕНИЕ УГРОЗ В ЦОД

23500

23800

ОБЗОР

Центры обработки данных нуждаются в высокой производительности, работоспособности и масштабируемости. Устройства 23000 сочетают в себе самые надежные средства защиты со специально разработанным оборудованием. Эти мощные устройства безопасности оптимизированы для обеспечения пропускной способности в режиме предотвращения угроз на реальном трафике до 4,5 Гбит/с для обеспечения защиты наиболее важных активов.

Устройства Check Point 23000 идеально подходят для сетей центров обработки данных, которые требуют высокой производительности и гибкости параметров ввода-вывода. Если вы готовы перейти от 10 на 25, 40 или 100 GbE, то готовы и устройства 23000. Это 2U-устройства с пятью слотами расширения ввода-вывода для обеспечения высокой плотности портов, с резервными источниками питания переменного или постоянного тока, с дисковым массивом RAID1 2x 1ТБ (HDD) или 2x 480ГБ (SSD) и портом LOM для удаленного внеполосного управления.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast ZERO-DAY PROTECTION

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Модульная конструкция и широкий спектр сетевых опций, доступных в устройствах серии 23000, не только обеспечивают богатый набор возможностей подключения для этих шлюзов, но и делают их легко настраиваемыми для развертывания в любой сетевой среде.

Максимальные показатели	23500	23800
Производительность МСЭ (Гбит/с) [1]	34	43
Производительность предотвращения угроз (Гбит/с) [1]	2.9	3.6
Порты 1 GbE (медь)	42	42
Порты 10 GbE (оптоволокно)	20	20
Порты 40 GbE (оптоволокно)	4	4
Порты 100/25 GbE (оптоволокно)	4	4
ОЗУ	128 ГБ	128 ГБ
Система хранения	2x 1ТБ (HDD) или 2x 480ГБ (SSD)	
Источники питания переменного или постоянного тока	2	2
Внеполосное управление LOM	✓	✓
Виртуальные системы	125	250

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/data-center-enterprise-security/

СИСТЕМЫ БЕЗОПАСНОСТИ 44000, 64000

МАСШТАБИРУЕМАЯ МНОГОМОДУЛЬНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

СИСТЕМЫ БЕЗОПАСНОСТИ 44000 И 64000

ОБЗОР

Когда речь заходит о защите самых требовательных сетевых сред центров обработки данных, провайдеров телекоммуникационных и облачных услуг, безопасность и производительность - это два важных требования, которые должны быть обеспечены одновременно. Модульная архитектура аппаратного и программного обеспечения в системах безопасности 44000 и 64000 идеально подходит для этих сред. Платформа обеспечивает масштабируемую пропускную способность межсетевого экрана на реальном трафике до 240 Гбит/с у 44000 и до 539 Гбит/с на платформе 64000.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast ZERO-DAY PROTECTION

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Разработанное с нуля для обеспечения надежности, доступности и удобства обслуживания центров обработки данных и сервис-провайдеров, шасси ATCA операторского класса работает в режимах высокой доступности и распределения нагрузки между модулями шлюза безопасности в одном шасси. Добавьте еще одно шасси, работающее в режиме высокой доступности, чтобы еще больше улучшить резервирование – обеспечить доступность и защиту критически важных активов.

Maximum Capacities	44000	64000
Производительность МСЭ (Гбит/с) [1]	до 240	до 539
Порты 100 GbE (оптоволокно)	до 4	до 4
Порты 40 GbE (оптоволокно)	до 12	до 12
Порты 10 GbE (оптоволокно)	до 64	до 64
Модули коммутатора безопасности	от 1 до 2	2
Модули шлюза безопасности	от 1 до 6	от 2 до 12
Источники питания	4 переменный ток	6 переменный ток

[1] Производительность при использовании реального трафика, типовой базы правил, NAT и включенным журналированием, а также наиболее безопасном предотвращении угроз

Подробная информация: www.checkpoint.com/products/high-performance-scalable-platforms/

ВИРТУАЛЬНЫЕ ШЛЮЗЫ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ ОБЛАКОВ

Широкое внедрение облачных архитектур – будь то публичных, частных или гибридных – обусловлено стремлением преобразовать предприятие для большей эффективности, скорости, гибкости и контроля за затратами. Хотя облако обладает многими преимуществами по сравнению с традиционной инфраструктурой, оно также ставит перед вашей компанией целый ряд задач безопасности. Check Point предлагает полный набор решений по безопасности публичных и частных облаков, который беспрепятственно расширяет защиту для любой облачной среды, так что вы можете быть уверены в облаке, как и в своей физической среде.

БЕЗОПАСНОСТЬ ПУБЛИЧНЫХ IaaS

Когда вы перемещаете вычислительные ресурсы и данные в публичное облако, обязанности по обеспечению безопасности распределяются между вами и вашим провайдером облачных услуг. Потеря контроля над перемещением приложений и данных из предприятия облачным провайдером, таким как веб-сервисы Amazon или Microsoft Azure, и возникающие при этом проблемы в мониторинге и управлении этими ресурсами создают различные проблемы безопасности. Это особенно верно из-за анонимного, многопользовательского характера публичного облака. Многие компании используют гибридные облака для поддержания контроля над своей частной облачной инфраструктурой и защиты конфиденциальных активов, а также аутсорсинг других аспектов в публичных облаках. С гибридным облаком новая задача заключается в защите данных при их перемещении от предприятия до публичного облака и обратно.

Check Point CloudGuard обеспечивает автоматизированную и гибкую защиту активов и данных при сохранении согласованности с динамическими характеристиками публичных облачных сред.

Amazon Web Services

Microsoft Azure

VMware Cloud on AWS

Alibaba Cloud

Oracle Cloud

БЕЗОПАСНОСТЬ ЧАСТНЫХ IaaS

Поскольку предприятия используют программно-определяемые сети и частные облачные среды, повышенная гибкость и эффективность поначалу воспринимались как благо для бизнеса, но привели к резкому увеличению сетевого трафика, идущего «горизонтально», внутри центра обработки данных. Этот сдвиг в структурах трафика создает новые проблемы безопасности. Благодаря ограниченному количеству элементов управления для «горизонтального» трафика угрозы могут беспрепятственно перемещаться внутри центра обработки данных.

Check Point CloudGuard обеспечивает динамическую безопасность в виртуальных центрах обработки данных для предотвращения «горизонтального» распространения угроз при консолидации обзора и управления в физических и виртуальных сетях.

Cisco ACI

VMware NSX

OpenStack

Virtual Edition NGFW

Подробная информация: www.checkpoint.com/products/cloud-security/

УСТРОЙСТВА SMART-1

УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ В ЭПОХУ БОЛЬШИХ ДАННЫХ


405


410


525


5050


5150

ОБЗОР

Растущие сети, прорывные технологии и распространение взаимоподключенных устройств требуют нового подхода к управлению безопасностью. Архитектура Check Point Infinity консолидирует управление несколькими уровнями безопасности, обеспечивая превосходную эффективность политик и позволяя управлять безопасностью через единую панель на экране. Единое управление централизованно коррелирует все типы событий во всех сетевых средах, облачных сервисах и мобильных инфраструктурах.

Чтобы эффективно управлять средой безопасности, организациям нужны такие решения по управлению безопасностью, которые эффективны, обрабатывают больше данных и делают это быстрее, чем когда-либо прежде. Устройства Check Point Smart-1 консолидируют управление безопасностью, включая ведение журнала, управление событиями и отчетность в единое специализированное устройство управления. Организации теперь могут эффективно отвечать требованиям к управлению данными и событиями в эпоху больших данных, получая централизованный обзор миллиардов журналов, визуальную индикацию рисков и способность быстро исследовать потенциальные угрозы.

УНИФИЦИРОВАННОЕ, ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

- УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ В ОДНОМ ДОМЕНЕ
- МУЛЬТИДОМЕННОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ
- МУЛЬТИДОМЕННОЕ УПРАВЛЕНИЕ ЖУРНАЛАМИ
- УПРАВЛЕНИЕ СОБЫТИЯМИ SMARTEVENT

ОБОБЩЕННЫЙ ОБЗОР

Организации могут использовать устройства Smart-1 для управления шлюзами в количестве от 5 до 5000. Благодаря мультидоменному управлению Smart-1 вы можете сегментировать сеть до 200 независимых доменов. Также устройства Smart-1 предоставляют до 48 ТБ встроенной системы хранения данных и до 256 ГБ оперативной памяти (ОЗУ).

Maximum Capacities	405	410	525	5050	5150
Управляемые шлюзы	5	10	25	50	150+
Макс. число доменов (мультидоменное управление)	×	×	×	50	200
Индексируемые журналы/сек	6,000	10,000	14,000	27,000	40,000
Установившееся число индексируемых журналов/сек	3,000	5,000	7,000	15,000	22,000
Размер журнала/день (ГБ)	53/1.7[1]	88/5.2[1]	150/17.1[1]	320/80[1]	470/128[1]
Жесткий диск	1x 1 ТБ	1x 2 ТБ	2x 4 ТБ	4x 4 ТБ	12x 4 ТБ
ОЗУ	16 ГБ	32 ГБ	64 ГБ	128 ГБ	256 ГБ
Блок питания с горячей заменой	×	×	✓	✓	✓

[1] Одно или Мультидоменная/выделенная конфигурация SmartEvent

Подробная информация: www.checkpoint.com/products/security-management-appliances/

УСТРОЙСТВА ЗАЩИТЫ ОТ DDOS

ОСТАНОВИТЬ «ОТКАЗ В ОБСЛУЖИВАНИИ» ЗА СЕКУНДЫ

506 / 1006 / 2006

4412 / 8412 / 12412

10420 / 20420 /30420 / 40420

ОБЗОР

В последние годы атаки типа «отказ в обслуживании» (DoS) и «распределенный отказ в обслуживании» (DDoS) возросли в количестве, сложности и скорости. Эти атаки относительно легко выполнить, и они могут нанести серьезный ущерб компаниям, которые полагаются в своей работе на веб-сервисы. Многие решения для защиты от DDoS развертываются провайдером интернет-услуг, обеспечивая общие меры защиты от сетевых атак. Однако сегодняшние атаки DDoS стали более сложными, включая в себя запуск нескольких атак на сетевом и прикладном уровнях. Успешные решения по защите от DDoS позволят компаниям настраивать свои механизмы защиты для того, чтобы отвечать меняющимся потребностям безопасности, быстрого времени отклика во время атаки и обеспечении выбора вариантов развертывания.

Устройства DDoS Protector предлагают гибкие варианты развертывания для обеспечения защиты бизнеса любого размера, интегрированное управление безопасностью для анализа трафика в реальном времени и управление анализом угроз для расширенной защиты от атак DDoS. Check Point также предоставляет выделенную круглосуточную поддержку 24/7 и ресурсы для обеспечения максимальной защиты.

МНОГОСЛОЙНЫЕ ЗАЩИТЫ

СЕТЕВОЙ ФЛУД И АТАКИ НА СТЕК TCP/IP

DOS/DDOS НА ОСНОВЕ ПРИЛОЖЕНИЙ

ОБОБЩЕННЫЙ ОБЗОР

Устройство Check Point DDoS Protector™ блокирует атаку «отказ в обслуживании» в течение нескольких секунд с помощью многослойной защиты и производительностью до 40 Гбит/с. DDoS Protector расширяет периметр безопасности компании, чтобы блокировать деструктивные атаки DDoS, прежде чем они нанесут ущерб.

Максимальные показатели	Enterprise	Data Center	Carrier
Производительность (Гбит/с) [1]	От 500 Мбит/с до 2 Гбит/с	От 4 до 12 Гбит/с	От 10 до 40 Гбит/с
Макс. количество одновременных сессий	2,000,000	4,000,000	6,000,000
Макс. темп предотвращения атаки DDoS типа «флуд» (пакетов в секунду)	1,000,000	10,000,000	25,000,000
Задержка	< 60 микросекунд		
10/100/1000 Copper Ethernet	4	8	
10 GbE (SFP+)			20
40 GbE QSFP			4
Сетевое функционирование	Прозрачная пересылка на 2 уровне модели OSI		
Высокая доступность	Активно-пассивный кластер		

[1] Производительность измерялась с включенными поведенческими и сигнатурными защитами IPS с использованием профиля защиты электронной коммерции

Подробная информация: www.checkpoint.com/products/ddos-protector/

УСТРОЙСТВА SANDBLAST

ПРЕДОТВРАЩЕНИЕ УГРОЗ «НУЛЕВОГО ДНЯ» ДЛЯ ЧАСТНОГО ОБЛАКА


TE100X


TE250X


TE1000X

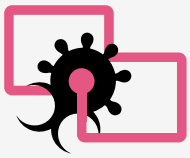

TE2000X

ОБЗОР

С увеличением сложности киберугроз многие целевые атаки начинаются с использования уязвимостей программного обеспечения в загружаемых файлах и вложениях электронной почты. Эти угрозы включают в себя новые эксплойты или даже варианты известных вредоносов, выпускаемых почти ежедневно, и к которым не существует сигнатур, а следовательно нет и стандартных решений для обнаружения этих вариантов вредоносного ПО. Новые и неизвестные угрозы требуют новых решений, выходящих за рамки сигнатур известных угроз.

Решение Check Point SandBlast Zero-Day Protection, защищенное от техник обхода, обеспечивает всестороннюю защиту даже от самых опасных атак, обеспечивая при этом быструю доставку безопасного контента вашим пользователям. В основе нашего решения лежат две уникальные технологии - Threat Emulation и Threat Extraction, которые обеспечивают защиту от угроз на новом уровне.

ОСТАНОВИТЬ НОВЫЕ И НЕИЗВЕСТНЫЕ УГРОЗЫ


THREAT EMULATION

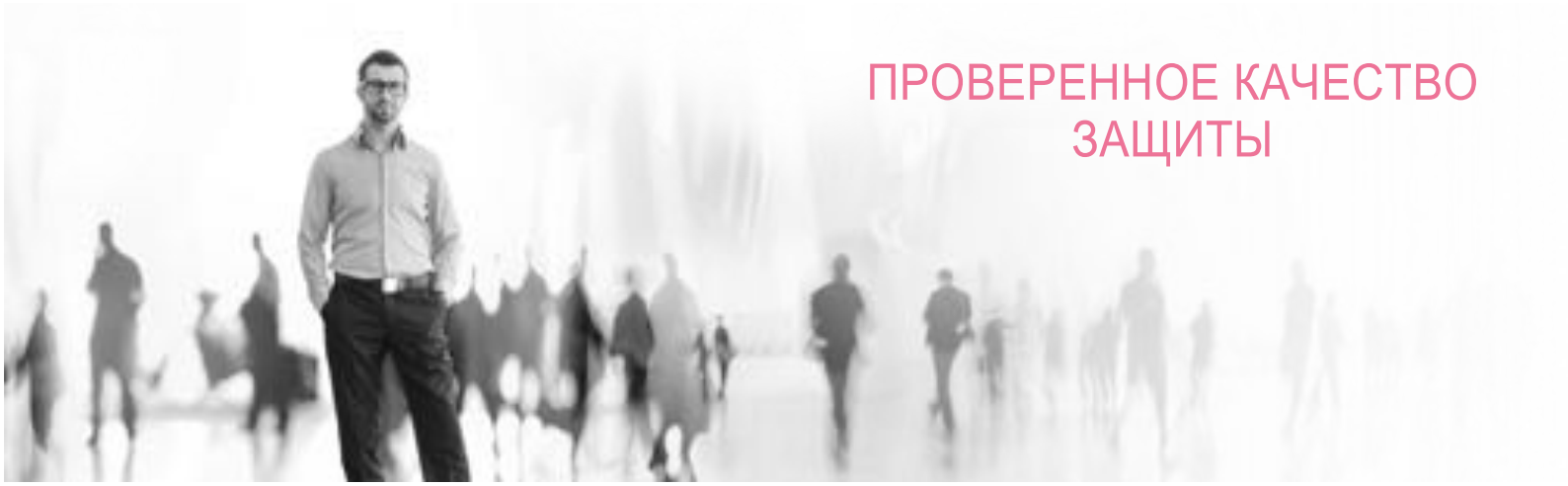

THREAT EXTRACTION

ОБОБЩЕННЫЙ ОБЗОР

Мы предлагаем широкий ассортимент устройств SandBlast. Они идеально подходят для клиентов, у которых есть задачи обеспечения требования регуляторов или конфиденциальности, которые не позволяют им использовать облачную службу SandBlast Threat Emulation.

Максимальные показатели	TE100X	TE250X	TE1000X	TE2000X
Рекомендованное число файлов /месяц	100 тыс.	250 тыс.	1 млн.	2 млн.
Рекомендованное число пользователей	до 1,000	до 3,000	до 10,000	до 20,000
Производительность	150 Мбит/с	700 Мбит/с	2 Гбит/с	4 Гбит/с
Число виртуальных машин	4	8	28	56
10/100/1000Base-T RJ45	13	17	14	14
10 ГBase-F SFP+	-	-	6	8
Корпус	1U	1U	2U	2U
Жесткий диск	1x 1ТБ		2x 2ТБ RAID1	
Источники питания	1	2	2	2

Подробная информация: www.checkpoint.com/products/sandblast-network-security/



ПРОВЕРЕННОЕ КАЧЕСТВО ЗАЩИТЫ

ПРИЗНАННЫЙ ЛИДЕР

Когда вы покупаете продукт Check Point, будьте уверены, что вы покупаете продукт у лидера индустрии безопасности и продукт, признанный ведущими тестирующими и аналитическими организациями.

GARTNER

СЕТЕВЫЕ МСЭ ПРЕДПРИЯТИЯ [1]

Лидер с 1997

GARTNER

УНИФИЦИРОВАННОЕ УПРАВЛЕНИЕ УГРОЗАМИ [2]

Лидер 6 лет подряд

NSS LABS

РЕКОМЕНДОВАНО В 14 ТЕСТАХ ПОДРЯД

- МСЭ
- МСЭ нового поколения
- IPS
- Системы обнаружения взлома (APT)

Дополнительные сертификации включают в себя: NATO Information Assurance Product Catalogue, Common Criteria Medium Robustness, Defense Information Systems Agency (Сертификация Министерства обороны США для МСЭ, VPN, IDS и IPS), Commercial Solutions for Classified Program, IPv6 Ready, VPN Consortium. Узнайте больше на сайте www.checkpoint.com.

[1] Gartner, Inc., Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, Greg Young, 25 May 2016.

[2] Gartner, Inc., Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hils, Greg Young, Rajpreet Kaur, 21 June 2017.

Свяжитесь с Check Point прямо сейчас

www.checkpoint.com/ru

Телефон/факс: +7 (495) 967 7444

E-mail: Russia@checkpoint.com

КОНТАКТЫ

Международная штаб-квартира | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

Представительство в Россиии и СНГ | Check Point Software Technologies (Russia) ООО | 109544, Москва, б-р Энтузиастов, 2, Деловой центр «Голден Гейт» | Тел./факс: +7 495 967 7444 | Эл. почта: Russia@checkpoint.com | www.checkpoint.com/ru

