Check Point®
SOFTWARE TECHNOLOGIES LTD.

Quantum

СЕТЕВАЯ БЕЗОПАСНОСТЬ

2021

СОДЕРЖАНИЕ

CHECK POINT
СЕТЕВАЯ БЕЗОПАСНОСТЬ

CHECK POINT
INFINITY

АРХИТЕКТУРА КИБЕРБЕЗОПАСНОСТИ БУДУЩЕГО

МОБИЛЬНЫЕ УСТРОЙСТВА | СЕТЬ | ОБЛАКО | КОНЕЧНЫЕ ТОЧКИ

СИТУАЦИЯ

По мере того как мир становится все более связанным сетями, а сети продолжают развиваться, защита IT-сред становится более сложной, чем раньше. Сейчас мы сталкиваемся с кибератаками Gen V (5-го поколения), крупномасштабными атаками, которые быстро распространяются, меняя векторы атак и отрасли промышленности. Атаки Gen V являются более сложными, чем когда-либо, они способны использовать различные мобильные, облачные и сетевые технологии, и обходить обычные средства защиты, основанные на обнаружении.

Раздельные IT-среды часто побуждают компании применять разные точечные решения, многие из которых сосредоточены на обнаружении и противодействии, а не на предотвращении. Этот реактивный подход к кибератакам дорогостоящ и неэффективен, усложняет работу системы безопасности и создает неустранимые пробелы в состоянии безопасности, оставляя вас незащищенными от сложных атак Gen V.

Пришло время перейти к поколению V кибербезопасности с архитектурой, которая действительно защитит всю вашу IT-инфраструктуру.

РЕШЕНИЕ

Check Point Infinity - единственная полностью консолидированная архитектура кибербезопасности, которая защищает ваш бизнес и IT-инфраструктуру от мега-кибератак Gen V во всех сетях, конечных точках, облаке и на мобильных устройствах.

Эта архитектура спроектирована для устранения сложностей растущих систем связи и неэффективной безопасности. Она обеспечивает полное предотвращение угроз, которое заполняет пробелы в защите, предоставляет автоматическое, немедленное совместное использование сведений об угрозах во всех средах и унифицированное управление безопасностью для максимально эффективного ее обеспечения. Check Point Infinity обеспечивает беспрецедентную защиту от текущих и потенциальных атак – сегодня и в будущем.

ЗАЩИТА ОТ УГРОЗ НОВОГО ПОКОЛЕНИЯ

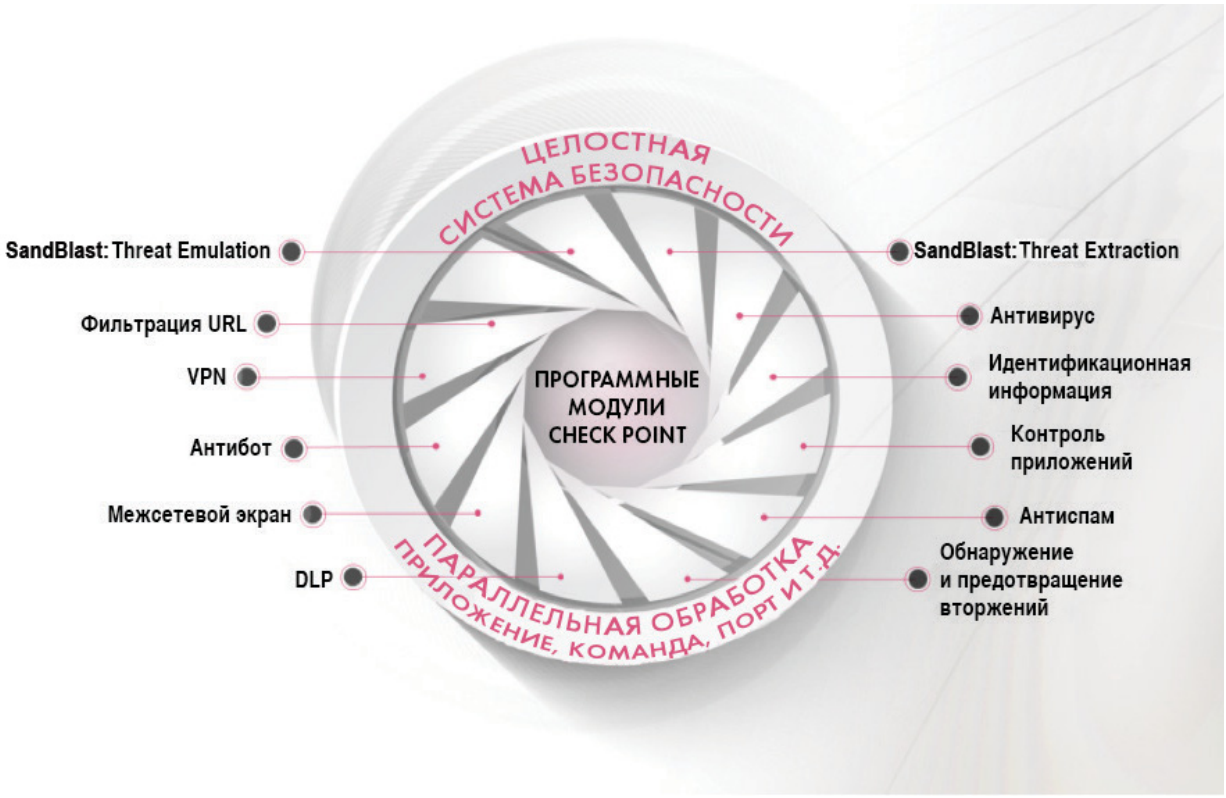
КОМПЛЕКСНОЕ ПРЕДОТВРАЩЕНИЕ УГРОЗ

Быстрый рост вредоносного ПО, растущее мастерство хакеров и появление новых неизвестных угроз «нулевого дня» требуют применения 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, контроль приложений 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»

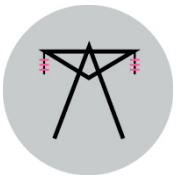
В рамках решения Check Point SandBlast Zero-Day Protection облачный механизм Threat Emulation обнаруживает вредоносное ПО на этапе эксплойта даже до того, как хакеры смогут применить методы уклонения, пытаясь обойти «песочницу» Файлы помещаются в карантин и проверяются путем запуска в виртуальной «песочнице», 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.

Более того, 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 безопасный контент пользователям, обеспечивая эффективность бизнес-процесса.



ШЛЮЗЫ БЕЗОПАСНОСТИ

Check Point предоставляет компаниям любых размеров новейшие решения по защите данных и сетевой безопасности на интегрированных платформах предотвращения угроз нового поколения, снижая сложность и 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.

 Модульные шасси	Размещение	ЦОД, Телко, Провайдеры	Maestro
	Форм-фактор	От 6RU	64000
	Интерфейсы	1, 10, 40, 100 GbE	44000
	Производительность	Пропускная способность предотвращения угроз от 90 до 1500 Гбит/с	
	Специфические особенности	Питание постоянного тока, кластеризация активный/активный	
 Центр обработки данных	Размещение	Большое предприятие, ЦОД	28000
	Форм-фактор	2RU	26000
	Интерфейсы	1, 10, 25, 40, 100 GbE	16200
	Производительность МСЭ	от 78.3 до 145 Гбит/с в тестовых условиях «Enterprise» (предприятие)	
	Специфические особенности	25/40/100 GbE, питание постоянного тока, LOM	
 Предприятие	Размещение	Предприятие	7000, 6900
	Форм-фактор	1RU	6700, 6600
	Интерфейсы	1, 10, 40 GbE	6400, 6200
	Производительность МСЭ	от 9 до 48 Гбит/с в тестовых условиях «Enterprise» (предприятие)	
	Специфические особенности	Гибкость вариантов ввода-вывода, LOM	
 Филиал	Размещение	Филиал или малый офис	3800, 3600
	Форм-фактор	Настольный	1800, 1600
	Интерфейсы	1 GbE, Wi-Fi, DSL, 3G/4G/LTE	1500
	Производительность МСЭ	от 1 до 7.5 Гбит/с в тестовых условиях «Enterprise» (предприятие)	
	Специфические особенности	Веб-управление	
 Защищенное исполнение	Размещение	Агрессивные среды	1570R
	Форм-фактор	Настольный, DIN и настенный	
	Интерфейсы	1 GbE, поддержка 3G/4G/TE	
	Производительность МСЭ	4 Гбит/с	
	Специфические особенности	Питание постоянного/переменного тока	

QUANTUM MAESTRO

ГИПЕРМАСШТАБИРУЕМАЯ КООРДИНАЦИЯ ЗАЩИТЫ

Quantum Maestro Hyperscal Orchestrator 140 | 175

ОБЗОР

Check Point Maestro обеспечивает масштабируемость, гибкость и эластичность облака на площадке заказчика благодаря эффективной кластеризации N+1 на основе технологии Check Point HyperSync, максимально расширяющей возможности существующих шлюзов безопасности. Создайте свою собственную виртуализованную частную облачную площадку, совместив несколько шлюзов безопасности Check Point. Сгруппируйте их по набору функций безопасности, политике или активам, которые они защищают, и дополнительно виртуализируйте их с помощью технологии виртуальных систем.

С Maestro Hyperscale Orchestrator предприятия любого размера могут получить безопасность на уровне облака на своей площадке. Добавьте вычисления для удовлетворения ваших потребностей с помощью веб-интерфейса Maestro или RESTful API – и все это с минимальным риском простоя и максимальной эффективностью затрат.

ЭКОНОМИЧНОЕ МАСШТАБИРУЕМОЕ РАЗВЕРТЫВАНИЕ N+1

Эффективная кластеризация N+1 теперь доступна в рамках единой системы с Check Point Maestro. Когда шлюз добавляется в систему, его конфигурация, политика и версия программного обеспечения обновляются и согласовываются с существующей развернутой системой. В течение 6 минут новый шлюз становится активным участником, увеличивая общую емкость системы.

Например, развернув нашу модель 16600HS вы можете начать с одного шлюза, обеспечивающего пропускную способность предотвращения угроз 17.6 Гбит/с. Затем легко добавьте существующие и новые шлюзы и создайте решение безопасности, обеспечивающее пропускную способность до 850 Гбит/с для предотвращения угроз, просто используя Check Point Maestro.

QUANTUM 64000, 44000

МАСШТАБИРУЕМАЯ МНОГОМОДУЛЬНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

Quantum
Scalable Chassis

QUANTUM 64000, 44000

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 до 335 Гбит/с у 44000 и до 800 Гбит/с на платформе 64000.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™

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.

Максимальные показатели	44000	64000
Производительность МСЭ (Гбит/с)[1]	до 90	до 180
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 переменного тока	6 переменного или 2 постоянного тока

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

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

QUANTUM 28000, 26000

ПРЕДОТВРАЩЕНИЕ УГРОЗ В ЦОД

Quantum Security Gateway

Quantum 26000, 28000

ОБЗОР

Шлюзы безопасности Check Point Quantum 26000 и 28000 сочетают в себе самые комплексные средства защиты и аппаратную платформу уровня ЦОД, чтобы максимизировать время безотказной работы и производительность для защиты крупных корпоративных сред и центров обработки данных. Устройства Check Point Quantum 26000 и 28000 идеально подходят для сетей центров обработки данных, которые требуют высокой производительности и гибкости параметров ввода-вывода.

Это 3U-устройства с восемью слотами расширения ввода-вывода для обеспечения высокой плотности портов, с резервными источниками питания переменного 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™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Максимальные показатели	26000	28000
Предотвращение угроз (Гбит/с)[1]	24	30
Производительность МСЭНП с IPS (Гбит/с)[1]	40.5	51.5
Порты 1 GbE (медь)	до 66x 10/100/1000 Base-T	
Порты 1, 10, 40 или 100/25 GbE (оптоволокно)	до 32x 1GbE, 32x 10GbE, 16x 40GbE или 16x 100/25 GbE	
Слоты расширения ввода-вывода	8	
ОЗУ	128 ГБ	
Система хранения	дисковый массив RAID1 2x 480GB SSD	
Источники питания переменного тока	3 резервных блока питания с возможностью горячей замены	
Внеполосное управление LOM	✓	

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

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

QUANTUM 16000

ПРЕДОТВРАЩЕНИЕ УГРОЗ ДЛЯ БОЛЬШИХ ПРЕДПРИЯТИЙ

Quantum Security Gateway

Quantum 16200

ОБЗОР

Шлюзы безопасности Check Point Quantum 16200 сочетают в себе комплексные средства защиты и аппаратную платформу уровня ЦОД, чтобы максимизировать время безотказной работы и производительность для защиты крупных корпоративных сред и центров обработки данных.

Устройства Check Point Quantum 16200 идеально подходят для крупных корпоративных сетей, которые требуют высокой производительности и гибкости параметров ввода-вывода. Это 2U-устройства с четырьмя слотами расширения ввода-вывода для обеспечения высокой плотности портов, с резервными источниками питания переменного тока, с дисковым массивом RAID1 2x 480ГБ (SSD) и портом LOM для удаленного внеполосного управления.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Максимальные показатели	16200
Предотвращение угроз (Гбит/с)[1]	15
Производительность МСЭНП с IPS (Гбит/с)[1]	27
Порты 1 GbE (медь)	до 34x 10/100/1000 Base-T
Порты 1, 10, 40 или 100/25 GbE (оптоволокно)	до 16x 1GbE, 16x 10GbE, 8x 40GbE или 8x 100/25 GbE
Слоты расширения ввода-вывода	4
ОЗУ	128 ГБ
Система хранения	дисковый массив RAID1 2x 480ГБ (SSD)
Источники питания переменного тока	2 резервных блока питания с возможностью горячей замены
Внеполосное управление LOM	✓

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

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

QUANTUM 7000

ПРЕДОТВРАЩЕНИЕ УГРОЗ ДЛЯ ПРЕДПРИЯТИЙ

Quantum
Security Gateway

Quantum 7000

ОБЗОР

У крупных предприятий высочайшие требования к производительности, времени безотказной работы и масштабируемости. Шлюзы безопасности Quantum 7000 сочетают самую полную и всестороннюю защиту со специализированным оборудованием. Эти мощные устройства безопасности оптимизированы для обеспечения пропускной способности предотвращения угроз до 9.5 Гбит/с, чтобы защищать ваши самые важные активы.

Устройства Check Point Quantum 7000 идеально подходят для корпоративных сетей, которые требуют высокой производительности и гибкости параметров ввода-вывода. Это 2U-устройства с двумя слотами расширения ввода-вывода для обеспечения высокой плотности портов, с резервными источниками питания переменного или постоянного тока, с дисковым массивом RAID1 2x 480ГБ (SSD) и портом LOM для удаленного внеполосного управления.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Модульная конструкция и широкий спектр сетевых возможностей, доступных в устройствах серии 7000, обеспечивают не только богатый набор вариантов подключения для этих шлюзов, но и их настраиваемость для развертывания в любой сетевой среде.

Максимальные показатели	7000
Предотвращение угроз (Гбит/с)[1]	9.5
Производительность МСЭНП с IPS (Гбит/с)[1]	22
Порты 1 GbE (медь)	26
Порты 10 GbE (оптоволокно)	8
Порты 40 GbE (оптоволокно)	4
ОЗУ	64 ГБ
Система хранения	дисковый массив RAID1 2x 480GB SSD
Источники питания переменного тока	2 резервных блока питания с возможностью горячей замены
Внеполосное управление LOM	✓

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

QUANTUM 6000

ПРЕДОТВРАЩЕНИЕ УГРОЗ ДЛЯ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ

Quantum Security Gateway

Quantum 6200, 6400

Quantum 6600, 6700

Quantum 6900

ОБЗОР

Решения безопасности больше не должны быть выбором между функционалом и производительностью. Специально разработанные устройства Check Point Quantum 6000 без компромиссов обеспечивают самую передовую защиту от угроз для корпоративных сетей малых и средних предприятий.

Устройства Quantum 6000, выполненные в компактном форм-факторе 1U, монтируемом в стойку, имеют в стандартной комплектации 10 портов 1 Gigabit Ethernet, и поддерживают резервные источники питания и модуль внеполосного управления LOM. Поддерживая до 17 Гбит/с пропускной способности МСЭ и 7.4 Гбит/с пропускной способности в режиме предотвращения угроз, эти устройства обеспечивают лучшую производительность в своем классе.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Один слот расширения в устройствах безопасности Quantum 6000, и два в серии 6900, обеспечивают богатый набор вариантов подключения для этих шлюзов.

Максимальные показатели	6200	6400	6600	6700	6900
Предотвращение угроз (Гбит/с)[1]	1.8	2.5	3.7	5.8	7.4
Производительность МСЭНП с IPS (Гбит/с)[1]	3.72	5.5	6.2	13.4	17
Порты 1 GbE (медь)	18				26
Порты 1 GbE (оптоволокно)	4				8
Порты 10 GbE (оптоволокно)	4				8
ОЗУ	32				64
Система хранения	1x 240ГБ SSD			1x 480ГБ SSD	2x 480ГБ SSD
Источники питания переменного тока	2 резервных источника питания				
LOM	✓				

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

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

QUANTUM 3000

БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ ДЛЯ ФИЛИАЛЬНЫХ ОФИСОВ

Quantum Security Gateway

Quantum 3600

Quantum 3800

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 Quantum 3600 и 3800 представляют собой идеальное решение для обеспечения безопасности в небольших офисах и филиалах.

Устройства Quantum 3600 и 3800 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 3 Гбит/с пропускной способности в режиме межсетевого экрана нового поколения (МСЭНП) и до 1.5 Гбит/с пропускной способности в режиме предотвращения угроз.

ПАКЕТЫ ВСЕОБЪЕМЛЮЩЕЙ БЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Компактная конструкция, многоядерные технологии и защита от угроз «нулевого дня» SandBlast, доступные в устройствах Quantum 3600 и 3800, делают эти шлюзы идеально подходящими для развертывания в небольших офисах и удаленных филиалах.

Максимальные показатели	3600	3800
Предотвращение угроз (Гбит/с)[1]	780 Мбит/с	1.5
Производительность МСЭНП с IPS (Гбит/с)[1]	1.5	3
Производительность VPN (Гбит/с)	2.71	2.75
ОЗУ	8 ГБ	16 ГБ
Порты 1 GbE (медь)	6	
Система хранения	1x 240ГБ SSD	
Корпус	Настольный	
Потребляемая мощность (макс.)	24.2 Вт	

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

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

QUANTUM SPARK™ 1600, 1800

СЕТЕВАЯ БЕЗОПАСНОСТЬ ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Quantum 1600

Quantum 1800

ОБЗОР

Обеспечение надежной сетевой безопасности на предприятии является сложной задачей для небольших и средних предприятий, где есть несколько пользователей, которые имеют малый опыт работы с IT. Офисы небольших и средних предприятий требуют такого же уровня защиты от сложных кибератак и угроз «нулевого дня», как и офисы крупных предприятий.

Шлюзы безопасности Check Point Quantum Spark 1600 и 1800 предоставляют защиту корпоративного класса в простых и доступных решениях «все в одном» в форм-факторе 1 RU (Rack Unit) для защиты сотрудников, сетей и данных компаний малого и среднего бизнеса от киберкраж. Предлагая высокую пропускную способность предотвращения угроз и большую емкость портов с сетевыми интерфейсами 2.5 и 10 GbE в серии 1800, эти МСЭНП являются идеальными решениями для сетей крупных филиалов и компаний малого и среднего бизнеса.

ВСЕОБЪЕМЛЮЩАЯ БЕЗОПАСНОСТЬ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

Check Point SandBlast™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

В стандартной конфигурации шлюзы серий 1600 и 1800 поставляются с шестнадцатью портами коммутатора LAN 1-Gigabit Ethernet и портом WAN 1-GbE, поддерживающим медные и оптоволоконные подключения. Порт DMZ является комбинированным медным/оптоволоконным портом 1 GbE в серии 1600 и 10 GbE в серии 1800. Серия 1800 имеет два дополнительных порта LAN 2.5 GbE и два блока питания для целей резервирования.

Максимальные показатели	1600	1800
Предотвращение угроз[1]	1.5 Гбит/с	2 Гбит/с
МСЭНП + IPS	3.2 Гбит/с	5 Гбит/с
Порты LAN	16 медных портов 1GbE	16 медных портов 1GbE и 2 медных порта 2.5GbE
Порты WAN	1 медный/оптоволоконный порт 1GbE	2 медных/оптоволоконных порта 1GbE
Порты DMZ	1 медный/оптоволоконный порт 1GbE	1 медный/оптоволоконный порт 10GbE
Источники питания	1	2 резервных
Система хранения	32 ГБ eMMC и дополнительно 64 ГБ карта памяти MicroSD	32 ГБ eMMC и 256 ГБ SSD

[1] Измерения проводились в тестовых условиях «Enterprise» (предприятие).

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

QUANTUM SPARK™ 1500

БЕЗОПАСНОСТЬ МАЛЫХ ОФИСОВ

Quantum Spark 1530/1550 Wi-Fi

Quantum Spark 1570/1590 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 Quantum Spark 1500 – 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.

Устройства Quantum Spark 1500 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 на своей площадке или в облаке для удаленного управления и единообразного применения политики безопасности для тысяч устройств на местах.

ВСЕОБЪЕМЛЮЩАЯ БЕЗОПАСНОСТЬ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Доступные в четырех вариантах, 1530/1550 и 1570/1590, эти устройства поставляются в стандартной комплектации с шестью (6) или десятью (10) портами 1-Gigabit Ethernet соответственно. Обеспечивается безопасное подключение с любого устройства напрямую или через Wi-Fi с безопасной аутентификацией.

Максимальные показатели	1530	1550	1570	1590
Предотвращение угроз	340 Мбит/с	450 Мбит/с	500 Мбит/с	660 Мбит/с
МСЭНП + IPS	600 Мбит/с	800 Мбит/с	970 Мбит/с	1,300 Мбит/с
Порты 1 GbE	1x WAN, 5x коммутатор LAN		1x WAN, 1x DMZ, 8x коммутатор LAN	
Оптический порт 1 GbE DMZ	-		1x 1000BaseF SFP порт	
Вариант Wi-Fi	802.11 b/g/n/ac, одинарный диапазон 2.4 или 5GHz		802.11 n/ac, двойной диапазон 2.4 и 5GHz	
Вариант DSL	x		✓	
Вариант LTE	x		✓	
Число мобильных пользователей (по умолчанию)	100		200	

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

QUANTUM RUGGED

БЕЗОПАСНОСТЬ ДЛЯ АГРЕССИВНЫХ СРЕД

Quantum Security Gateway

Quantum Rugged 1570R

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 Quantum Rugged 1570R дополняет наше обширное семейство устройств для поддержки разнообразных сред развертывания и удовлетворения особых требований. Например, 1570R 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

Check Point SandBlast™

ПРЕДОТВРАЩЕНИЕ УГРОЗ + SANDBLAST

ОБОБЩЕННЫЙ ОБЗОР

Медные и оптоволоконные Ethernet-порты 1GbE, а также дополнительно Wi-Fi и встроенный беспроводной модем 3G/4G/LTE.

Максимальные показатели	1570R
Производительность предотвращения угроз	400 Мбит/с
Производительность МСЭНП	700 Мбит/с
WAN	1x 10/100/1000BaseT RJ45 или 1x 1000BaseF порт
DMZ	1x 10/100/1000BaseT RJ45 или 1x 1000BaseF порт
LAN	Порты 8x 10/100/1000BaseT RJ45
Варианты установки	Рейка DIN или крепление на стену
Сертификации	Промышленность, судоходство, прочность (удары и вибрация), класс защиты IP30
Диапазон рабочих температур	40°C – 75°C (-40°F – +167°F)

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

ВИРТУАЛЬНЫЕ УСТРОЙСТВА

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 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.

CloudGuard Network

Amazon Web Services

CloudGuard Network

Microsoft Azure

CloudGuard Network

VMware Cloud on AWS

CloudGuard Network

Google Cloud Platform

CloudGuard Network

Alibaba Cloud

CloudGuard Network

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.

CloudGuard Network

Cisco ACI

CloudGuard Network

VMware NSX

CloudGuard Network

OpenStack

CloudGuard Network

Virtual Edition NGFW

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

QUANTUM SMART-1

УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ В ЭПОХУ БОЛЬШИХ ДАННЫХ


600-S


600-M


6000-X


6000-XL

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 в сетевых, облачных и мобильных средах, 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 384 ГБ оперативной памяти (ОЗУ).

Максимальные показатели	600-S	600-M	6000-X	6000-XL
Управляемые шлюзы	10	50	150	400+
Макс. число доменов (мультидоменное управление)	x	x	50	200
Индексируемые журналы/сек (пиковое значение)	70,000	90,000	38,000	60,000
Установившееся число индексируемых журналов/сек	8,000/2,000[1]	13,000/4,000[1]	23,000/23,000[1]	40,000/40,000[1]
Размер журнала/день (ГБ)	200/50[1]	295/105[1]	616/38[1]	999/65[1]
Система хранения	1x 2ТБ HDD	2x 4ТБ HDD	12x 4ТБ B HDD	12x 4ТБ SSD
ОЗУ	32 ГБ	64 ГБ	192 ГБ	384 ГБ
Блок питания с горячей заменой	x	✓	✓	✓

[1]600-S и 600-M протестированы с конфигурацией SmartLog и SmartEvent, 6000-L/6000-XL протестированы со специальной конфигурацией SmartEvent

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

УСТРОЙСТВА ЗАЩИТЫ ОТ DDOS

ОСТАНОВИТЬ «ОТКАЗ В ОБСЛУЖИВАНИИ» ЗА СЕКУНДЫ

6

20 / 60

110 / 220

200 / 400

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 требованиям 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 быстрой и 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 400 Гбит/с. DDoS Protector расширяет периметр безопасности компании, чтобы блокировать деструктивные атаки DDoS, прежде чем они нанесут ущерб.

Максимальные показатели	6	20	60	110	200	220	400
Полоса пропускания	6	20	60	110	200	220	400
Макс. темп предотвращения атаки DDoS типа «флуд» (пакетов в секунду)	5.8 млн.	25 млн.	25 млн.	50 млн.	330 млн.	146 млн.	330 млн.
Количество SSL/TLS соединений в секунду (RSA 2K)	20 тыс.	95 тыс.	95 тыс.	150 тыс.	-	150 тыс.	-
Задержка	< 60 микросекунд						
Сетевое функционирование	Прозрачная L2-переадресация/ IP-переадресация						
Варианты развертывания	«В линии», SPAN-порт, копирование порта, гибридное (опция центра очистки в облаке)						
Порты	8x RJ45, 2x 1/10 GbE	24x 1/10 GbE		24x 10, 8x 40, 4x 100 GbE	20x 10, 4x 40, 4x 100 GbE	24x 10, 8x 40, 4x 100 GbE	20x 10, 4x 40, 4x 100 GbE
Корпус	1U	2U	2U	2U	2U	2U	2U

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, предоставляет 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

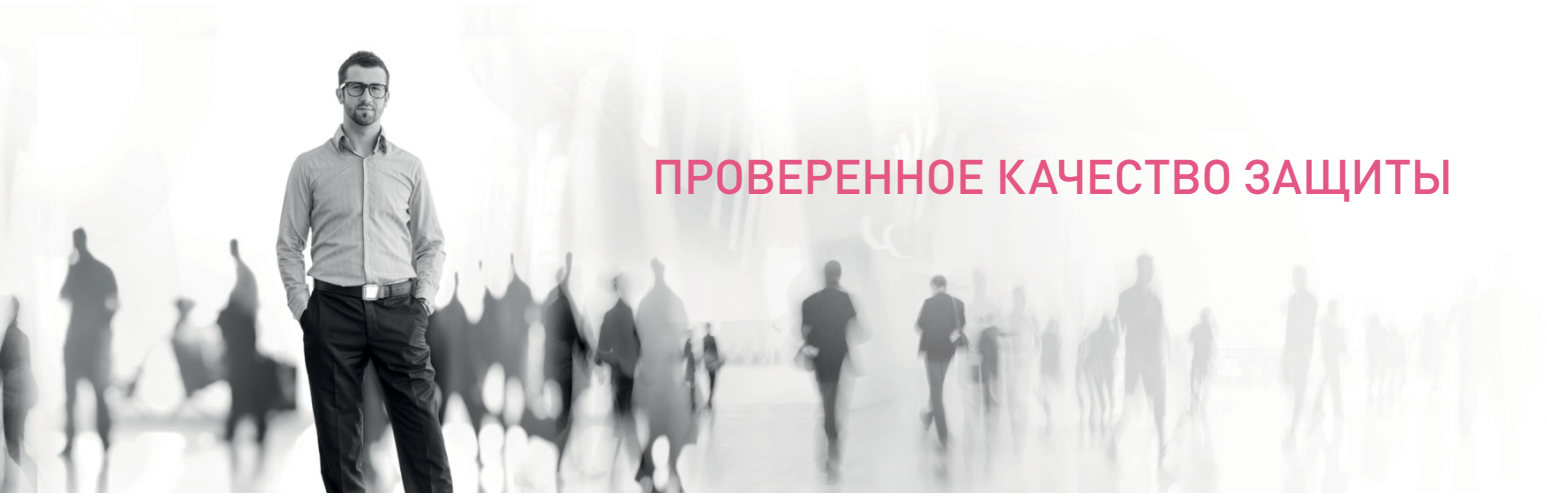
THREAT EXTRACTION

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
Число уникальных файлов/час	450	1,000	2,800	5,000
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
10GBase-F SFP+	-	-	6	8
Байпасные порты (Fail-Open)	Дополнительные порты 4x 1GbE медные или 2x 10GbE			
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.

ЛИДЕР МАГИЧЕСКОГО КВАДРАНТА GARTNER ДЛЯ РЫНКА МЕЖСЕТЕВЫХ ЭКРАНОВ В 2020 ГОДУ

21x

Check Point Software Technologies с гордостью сообщает, что по результатам исследования «Магический квадрант для рынка межсетевых экранов в 2020 году» компания была названа лидером рынка. Gartner признает нас лидером уже в 21-й раз. В ходе своего ежегодного исследования Gartner проводит анализ рынка, тщательно тестирует решения поставщиков — и помещает лучших из них в сектор лидеров. Благодаря надежной архитектуре Infinity и сосредоточенности на защите облачных сред, мы укрепили свою позицию в отчете 2020 года, получив высокие оценки за производительность, надежность предотвращения угроз и интеграцию продуктов. Мы отличаемся своими инновационными средствами централизованного управления безопасностью, эффективным управлением политиками и передовой технологией предотвращения угроз.

СТАТУС NSS LABS RECOMMENDED

NSS Labs RECOMMEND

С 2011 года Check Point принимает активное участие в тестах NSS Labs и получила статус NSS Labs Recommended в таких категориях, как межсетевой экран, межсетевой экран нового поколения, системы предотвращения вторжений (IPS) и системы предотвращения нарушений безопасности (BPS). В отчете NSS Labs 2019 года компания Check Point получила наивысшую оценку по эффективности средств защиты BPS, которая имеет большое значение, поскольку охватывает множество решений, позволяющих поставщику обеспечивать своим клиентам предотвращение нарушений безопасности. Использование нескольких решений обеспечивает синергию между различными компонентами защиты, сочетание которых эффективно блокирует кибератаки на всех их этапах. В случае Check Point решение включало множество технологий, в том числе SandBlast Network, SandBlast Agent, Threat Extraction, антибот и другие.

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED IPSEC - BASIC

FIPS VALIDATED 140-2

Common Criteria

Другие сертификаты: NATO Information Assurance Product Catalogue, Common Criteria Medium Robustness, Defense Information Systems Agency (сертификаты Министерства обороны США для межсетевого экрана, VPN, IDS и IPS), Commercial Solutions for Classified Program, IPv6 Ready, VPN Consortium. Дополнительную информацию можно получить на сайте www.checkpoint.com.

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, Jeremy D'Hoinne, 9 ноября 2020 г.

Свяжитесь с Check Point прямо сейчас

CIS@checkpoint.com

г. Алматы, ул. Тимирязева 26/29, Бизнес-центр «BNC Plaza»

г. Киев, ул. Пимоненко 13, Бизнес-центр «Форум», офис 6А-27

Check Point®
SOFTWARE TECHNOLOGIES LTD.