Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

2200

Решение для филиала и малого офиса — корпоративная безопасность в настольном исполнении

Устройство Check Point 2200

Сегодня шлюз компании — это больше, чем просто межсетевой экран. Это устройство безопасности, отвечающее возрастающему числу сложных угроз. Выступая в качестве шлюза безопасности, он должен использовать различные технологии для контроля доступа к сети, обнаруживать сложные атаки и предоставлять дополнительные возможности защиты, такие как предотвращение потери данных и защита от интернет-угроз. Распространение мобильных устройств, таких как смартфоны и планшеты, новых приложений для социальных сетей, потоковой передачи данных, пиринговых приложений требует большей пропускной способности каналов связи и новых технологий управления приложениями. Наконец, переход компании к собственным и публичным облачным сервисам, во всех его вариациях, изменяет границы компании и требует расширения возможностей и дополнительных решений в области безопасности.

Новые устройства компании Check Point объединяют в себе высокоскоростные сетевые технологии с высокопроизводительными характеристиками, основанными на использовании многоядерности процессора, обеспечивая высочайший уровень безопасности без ущерба для быстродействия сети, так что ваши данные, сеть и работники защищены. Оптимизированное под Архитектуру «Программные блейды», каждое устройство может работать с любой комбинацией Программных блейдов, обеспечивая гибкость и определенный уровень защиты для любой компании в любом месте сети путем объединения нескольких технологий защиты в единое комплексное решение.

Каждое устройство Check Point поддерживает концепцию безопасности Check Point 3D Security, сочетающую политики, людей и принуждение с целью непревзойденной защиты. Для удовлетворения изменяющихся потребностей в области безопасности, компания Check Point предлагает пакеты Next Generation Security на основе Программных блейдов, ориентированные на конкретные требования заказчика. Технологии Threat Prevention, Data Protection, Web Security и Next Generation Firewall являются ключевыми основами для надежного проекта 3D Security.

ОБЗОР

Устройство Check Point 2200 представляет собой компактное настольное устройство, основанное на использовании многоядерной технологии. Для высокой пропускной способности сети в устройстве 2200 имеется шесть встроенных портов 1 Gigabit Ethernet (витая пара). Несмотря на свой небольшой размер, это мощное устройство обеспечивает приличный показатель SecurityPower в 114 единиц, пропускную способность межсетевого экрана 3 Гбит/с и IPS более 2 Гбит/с. Эффективное и доступное полнофункциональное решение в области безопасности идеально подходит для защиты небольших филиалов.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- 114 SecurityPower™
- Пропускная способность межсетевого экрана 3 Гбит/с
- Пропускная способность IPS 2 Гбит/с
- 6 портов 10/100/1000Base-T
- Настольное исполнение

ПРЕИМУЩЕСТВА

- Доверяют 100% из списка Fortune 100
- Комплексное устройство защиты
- Единая консоль управления
- Гарантируется защита данных с VPN
- Расширяемая Архитектура «Программные блейды»

ПРОГРАММНЫЕ БЛЕЙДЫ ШЛЮЗА

	FW	NGFW	NGDP	NGTP
Firewall	■	■	■	■
IPsec VPN	■	■	■	■
Mobile Access (5 пользова-телей)	■	■	■	■
Advanced Networking & Clustering	■	■	■	■
Identity Awareness	■	■	■	■
IPS	*	■	■	■
Application Control	*	■	■	■
Data Loss Prevention	*	*	■	*
URL Filtering	*	*	*	■
Antivirus	*	*	*	■
Anti-spam	*	*	*	■
Anti-Bot	*	*	*	■

* Опционально

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

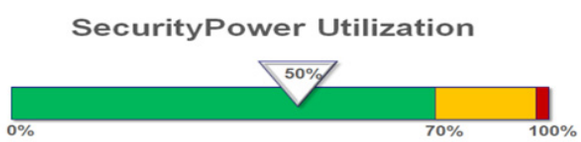
2200

1. Установка в стойку на полку (опционально)
2. 6 портов 10/100/1000Base-T RJ45
3. Два USB-порта для установки ISO
4. Консольный порт RJ45

SECURITYPOWER™

До сих пор выбор устройства защиты был основан на выборе конкретных показателей эффективности для каждой функции безопасности, как правило, в лабораторных испытаниях при оптимальных условиях и с использованием политики безопасности, которая содержит одно правило. Сегодня клиенты могут выбрать устройства защиты на основе рейтинга SecurityPower™, который рассчитан на реальном трафике пользователя, множестве функций безопасности и типовой политике безопасности.

SecurityPower это новый эталонный тест, который измеряет способность и мощность устройства при работе с несколькими дополнительными функциями безопасности (Программными блейдами), такими как IPS, DLP и Application Control, в условиях передачи реального трафика. Это обеспечивает эффективную метрику для более точного прогнозирования текущего и будущего поведения техники при противодействии атакам и в ежедневной работе. Технические требования SecurityPower Unit (SPU), определенные с использованием Check Point Appliance Selection Tool, могут быть сопоставлены с SPU устройств Check Point, что позволяет выбрать подходящее устройства в соответствии с конкретными требованиями заказчика.



КОМПЛЕКСНОЕ РЕШЕНИЕ В ОБЛАСТИ БЕЗОПАСНОСТИ

Устройство Check Point 2200 представляет собой готовое, консолидированное решение в области безопасности в компактном настольном исполнении. Основанное на Check Point Архитектуре «Программные блейды», устройство доступно в виде четырех пакетов Программных блейдов и имеет расширяемую архитектуру, чтобы совершенствовать защиту за счет включения дополнительных Программных блейдов.

- **Firewall (FW):** создает контролируемые (в разрезе пользователей) и защищенные соединения с корпоративными сетями для удаленных и мобильных пользователей, филиалов и деловых партнеров с помощью IPsec VPN.
- **Next Generation Firewall (NGFW):** идентифицирует и контролирует приложения на основе пользователя и сканирует содержимое, чтобы остановить угрозы — с блейдами IPS и Application Control.
- **Next Generation Data Protection (NGDP):** превентивная защита конфиденциальной информации от непреднамеренной потери, обучает пользователей надлежащей политике обработки данных и позволяет устранять инциденты в режиме реального времени — с блейдами IPS, Application Control и DLP.
- **Next Generation Threat Prevention (NGTP):** использует несколько уровней защиты для предотвращения кибер-угроз — с блейдами IPS, Application Control, Antivirus, Anti-Bot, URL Filtering и Email Security.

ПРЕДОТВРАЩЕНИЕ НЕИЗВЕСТНЫХ УГРОЗ С ЭМУЛЯЦИЕЙ THREATCLOUD

Устройства Check Point являются ключевыми компонентами в экосистеме ThreatCloud, обеспечивая превосходную защиту от неизвестных вредоносных кодов, целенаправленных атак и атак нулевого дня. Устройства проверяют и отправляют подозрительные файлы в Службу эмуляции ThreatCloud, которая исполняет их в виртуальной выделенной изолированной среде для обнаружения вредоносного поведения. Выявленное вредоносное ПО не допускается в сеть. Создается сигнатура и отправляется в базу знаний ThreatCloud, которая распространяет информацию о вновь выявленной угрозе для защиты других клиентов Check Point.

ИНТЕГРИРОВАННОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

Устройством можно управлять как локально, с помощью интегрированного управления безопасностью, так и с единой консоли управления. С использованием локального управления, можно управлять самим устройством и одним соседним устройством в целях обеспечения высокой готовности.

GAIA — ЕДИНАЯ ОС БЕЗОПАСНОСТИ

Check Point GAiA™ является следующим поколением защищенных операционных систем для всех устройств Check Point, открытых серверов и виртуальных шлюзов. GAiA сочетает в себе лучшие черты IPSO и SecurePlatform в единой унифицированной ОС, которая обеспечивает превосходную эффективность и высокую производительность. Обновляя до GAiA, клиенты получают преимущества в виде расширенных возможностей подключения устройства и снижения расходов

в эксплуатации. С GAiA, клиенты получают возможность использовать всю широту и мощь Программных блейдов Check Point. GAiA обеспечивает безопасность сетей IPv4 и IPv6, использующих технологию Check Point Acceleration & Clustering и защищает более сложные сетевые среды за счет поддержки протоколов динамической маршрутизации, таких как RIP, OSPF, BGP, PIM (Sparse mode и Dense mode) и IGMP. В 64-разрядных ОС, GAiA увеличивает емкость соединений выбранных устройств.

Ролевой административный доступ для разделения полномочий в GAiA упрощает управление. Кроме того, GAiA значительно повышает эффективность работы, предлагая автоматическое обновление ПО. Наглядный и многофункциональный web-интерфейс позволяет осуществлять мгновенный поиск любой команды или свойства. GAiA имеет полную совместимость с интерфейсом командной строки IPSO и SecurePlatform, что облегчает переход клиентов Check Point на новую ОС.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Базовая конфигурация
6 портов 10/100/1000Base-T RJ45
Жесткий диск емкостью 250G
Внешний адаптер с переменного в постоянное напряжение
Производительность продукта [1]
114 SecurityPower
Пропускная способность межсетевого экрана 1.4 Гбит/с
Пропускная способность межсетевого экрана и IPS 150 Мбит/с
Тесты производительности (LAB) RFC 3511, 2544, 2647, 1242
Пропускная способность межсетевого экрана 3 Гбит/с, 1518 байт UDP
Пропускная способность VPN 400 Мбит/с, AES-128
Максимум 20,000 туннелей IPsec VPN
Пропускная способность IPS 2 Гбит/с. Профиль IPS по умолчанию, смесь трафика IMIX
Пропускная способность IPS 300 Мбит/с. Рекомендованный профиль IPS, смесь трафика IMIX
1.2 миллиона одновременных соединений, 64-байтный HTTP-ответ
25,000 соединений в секунду, 64-байтный HTTP-ответ
Network Connectivity
IPv4 и IPv6
1024 интерфейса или VLANs на систему
4096 интерфейсов на систему (в режиме Виртуальной системы)
802.3ad пассивная и активная агрегация каналов
Layer 2 (прозрачный) и Layer 3 (маршрутизации) режим
Высокая готовность
Активный/Активный – L3 режим
Активный/Пассивный – L3 режим
Синхронизация сессий для межсетевого экрана и VPN
Перехват управления сессией при изменении маршрутов
Обнаружение неисправности устройства
ClusterXL или VRRP
Обнаружение обрыва соединения

Виртуальные системы
Max VSs: 3
Габаритные размеры
Корпус: Настольный
Стандартные (W x D x H): 8.27 x 8.25 x 1.65 дюймы
Метрические (W x D x H): 210 x 209.5 x 42 миллиметры
Масса: 2.0 кг. (4.4 фунта)
Требования по питанию
Входное питание AC: 100 – 240 В
Частота: 50-60 Гц
Номинальная мощность одного источника питания: 40 Вт
Максимальная потребляемая мощность: 35 Вт
Максимальный тепловой выход: 119.4 BTU
Условия окружающей среды в режиме работы
Температура: от 32° до 104°F / от 0° до 40°C
Влажность: 20%-90% (без конденсации)
Условия окружающей среды в режиме хранения
Температура: от –4° до 158°F / от –20° до 70°C
Влажность: от 5% до 95% @60°C (без конденсации)
Соответствие стандартам
Безопасность: CB, UL/cUL, CSA, TUV, NOM, CCC, IRAM, PCT/GoST
Излучение: FCC, CE, VCCI, C-Tick, CCC, ANATEL, KCC
Защищенность: RoHS

[1] Максимальная производительность продукта, основанная на эталонном тесте SecurityPower. Реальный трафик, несколько Программных блейдов, типичная база правил, активирован NAT и включена функция ведения журналов. Check Point рекомендует зарезервировать 50 % использования SPU для дополнительных Программных блейдов и будущего роста трафика. С помощью Appliance Selection Tool подберите подходящее устройство для работы исходя из собственных требований к обеспечению безопасности.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

СПЕЦИФИКАЦИИ ПАКЕТОВ ПРОГРАММНЫХ БЛЕЙДОВ

Базовые пакеты [1]	**SKU**
Устройство Check Point 2200 с блейдами FW, VPN, IA, ADNC и MOB-5 в комплекте с локальным управлением на 2 шлюза	CPAP-SG2205
Устройство 2200 Next Generation Firewall (включая блейды FW, VPN, ADNC, IA, MOB-5, IPS и APCL); в комплекте с локальным управлением на 2 шлюза	CPAP-SG2200-NGFW
Устройство 2200 Next Generation Data Protection (включая блейды FW, VPN, ADNC, IA, MOB-5, IPS, APCL и DLP); в комплекте с локальным управлением на 2 шлюза	CPAP-SG2200-NGDP
Устройство 2200 Next Generation Threat Prevention (включая блейды FW, VPN, ADNC, IA, MOB-5, IPS, APCL, URLF, AV, ABOT и ASPM); в комплекте с локальным управлением на 2 шлюза.	CPAP-SG2200-NGTP
Пакеты Программных блейдов [1]	**SKU**
Пакет Программных блейдов на 1 год для устройства 2200 NGFW (включая блейды IPS и APCL)	CPSB-NGFW-2200-1Y
Пакет Программных блейдов на 1 год для устройства 2200 NGDP (включая блейды IPS, APCL и DLP)	CPSB-NGDP-2200-1Y
Пакет Программных блейдов на 1 год для устройства 2200 NGTP (включая блейды IPS, APCL, URLF, AV, ABOT и ASPM)	CPSB-NGTP-2200-1Y
Дополнительные Программные блейды [1]	**SKU**
Программный блейд Mobile Access до 50 одновременных подключений	CPSB-MOB-50
Программный блейд Data Loss Prevention на 1 год (до 500 пользователей, до 15000 писем в час, максимальная пропускная способность 700 Мбит/с)	CPSB-DLP-500-1Y
Программный блейд IPS на 1 год	CPSB-IPS-S-1Y
Программный блейд Application Control на 1 год	CPSB-APCL-S-1Y
Программный блейд URL Filtering на 1 год	CPSB-URLF-S-1Y
Программный блейд Antivirus на 1 год	CPSB-AV-S-1Y
Программный блейд Anti-Spam & Email Security на 1 год	CPSB-ASPM-S-1Y
Программный блейд Anti-Bot на 1 год — для младших моделей устройств и предопределенных систем	CPSB-ABOT-S-1Y

[1] Доступны варианты Высокой готовности (HA) и другие на 2 и 3 года, см. в электронном Каталоге продуктов.

ПАКЕТЫ ВИРТУАЛЬНЫХ СИСТЕМ

Описание	**SKU**
Пакет на 3 Виртуальные системы	CPSB-VS-3
Пакет на 3 Виртуальные системы для HA/VSLS	CPSB-VS-3-VSLS

АКСЕССУАРЫ

Описание	**SKU**
Запасной блок питания постоянного напряжения для устройства 2200	CPAC-PSU-2200
Аксессуар для устройства 2200, один комплект для монтажа в стойку	CPAC-RM-2200

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com
Представительство в России и СНГ
Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444 | http://rus.checkpoint.com