ВИРТУАЛЬНЫЕ РЕШЕНИЯ WATCHGUARD XCSv

Использование виртуальных решений WatchGuard XCSv в сетевой инфраструктуре компании позволит:

- Получить новейшие технологии для защиты электронной почты и Web-трафика;
- Легкость установки, внедрения и управления;
- Возможности по управлению, как аппаратными, так и виртуальными решениями при помощи одной единой централизованной консоли;
- Использовать все преимущества и возможности виртуальной среды VSphere;
- Различные конфигурации виртуальных решений WatchGuard XCSv подойдут как для небольших компаний, так и для крупных компаний с большими потребностями в обеспечении информационной безопасности.

Виртуальные решения WatchGuard XCSv - это:

Виртуальные решения WatchGuard XCSv обладают лучшими в своем классе показателями по уровню блокирования спама и вирусов, а также имеют широчайшие возможности по предотвращению утечек конфиденциальных данных. Решения WatchGuard XCSv подойдут как для небольших компаний, так и для крупных компаний и позволяют обеспечить высокий уровень защиты сетевых ресурсов и конфиденциальной информации, а также добиться максимально высокого уровня соответствия нормативным требованиям. Множество компаний, для того чтобы сократить расходы и повысить эффективность работы своих ресурсов, все чаще обращают свое внимание на виртуальные решения. Одними из самых значимых приложений, на защиту которых стоит обратить особое внимание при переходе к виртуальной среде, являются электронная почта/ системы обмена мгновенными сообщениями (в том числе Microsoft Exchange), а также Web-приложения.

Виртуальные решения WatchGuard XCSv имеют лучшее среди всех производителей IPS решений соотношение «Цена – Производительность – Функционал - Качество» и обеспечивают высокий уровень защиты электронной почты, Web-трафика и данных, что позволяет предотвратить утечки конфиденциальных данных. Виртуальные решения WatchGuard XCSv обеспечивают непревзойденный уровень гибкости при внедрении. Решения WatchGuard XCSv могут быть развернуты в системах, которые содержат как аппаратные, так и виртуальные среды, и могут централизованно управляться из единой централизованной консоли управления.

ИНТЕГРАЦИЯ С ПОЧТОВЫМИ СЕРВЕРАМИ И СЕРВЕРАМИ ПРИЛОЖЕНИЙ ОБЕСПЕЧИВАЕТ БОЛЕЕ НАДЕЖНУЮ ЗАЩИТУ

Наиболее популярными приложениями, которые компании встраивают в свою виртуальную инфраструктуру, являются приложения обмена сообщениями (в том числе электронная почта), а также различные Web-приложения. По проведенным исследованиям наиболее популярной программой для использования в виртуальных средах является Microsoft Exchange. Решения WatchGuard XCSv позволяют защитить не только физическую инфраструктуру сети, но и виртуальную сетевую среду. Решения WatchGuard XCSv позволяют управлять всем входящим и исходящим сетевым трафиком, а широкие возможности при построении VPN туннелей обеспечивают безопасный доступ к корпоративным центрам обработки данных. В сочетании с высоким показателем гибкости при внедрении виртуальных решений и широкими возможностями централизованного управления, решения WatchGuard XCSv позволяют значительно сэкономить финансовые и материальные ресурсы, а также существенно повысить уровень сетевой безопасности.

КОНСОЛИДАЦИЯ НЕСКОЛЬКИХ РЕШЕНИЙ WATCHGURAD XCSv ЗНАЧИТЕЛЬНО ПОВЫШАЕТ ЭФФЕКТИВНОСТЬ

Поставщики услуг (например, хостинг провайдеры) могут развертывать несколько экземпляров виртуальных решений XCSv на серверах на периметре своей сети. Виртуальные решения WatchGuard XCSv изолированы друг от друга, так что изменение конфигурации одного межсетевого экрана не будет влиять на остальные виртуальные межсетевые экраны. Каждый экземпляр установленного решения WatchGuard XCSv может быть настроен независимо от других экземпляров, в том числе присутствует возможность индивидуальной настройки механизма обнаружения спама, который учитывает множество факторов обнаружения, в том числе лексику. Кроме этого все виртуальные решения WatchGuard XCSv могут управляться поставщиком услуг при помощи единой консоли централизованного управления.

Характеристики виртуальных решений WatchGuard серии XCSv

	Small Office	Medium Office	Large Office	Large Office XC
Требования к платформе				
Процессор (кол-во ядер)	1	2	4	8
Количество сетевых интерфейсов	2	3	4	4
Оперативная память (минимум)	2 Гб	2 Гб	4 Гб	8 Гб
Объем HDD (минимум)	64 Гб	104 Гб	184 Гб	280 Гб
Количество пользователей (рекомендуемое)	100	500	2000	5000
Функции безопасности				
Анти-спам/ Антивирус/ Блокирование вредоносного ПО	✔	✔	✔	✔
Блокирование смешанных угроз	✔	✔	✔	✔
Сервис «Reputation Enabled Defense» (RED)	✔	✔	✔	✔
Спам словари	✔	✔	✔	✔
Поддержка шаблонов для фильтров сообщений	✔	✔	✔	✔
Поддержка режима «Карантин»	✔	✔	✔	✔
Управление вложениями	✔	✔	✔	✔
Функции безопасности, доступные вместе с подпиской «Web Security»				
URL фильтрация	✔	✔	✔	✔
Сервис Web-репутации	✔	✔	✔	✔
Фильтрация Web контента	✔	✔	✔	✔
Контроль использования Web-ресурсов	✔	✔	✔	✔
Управление Web приложениями	✔	✔	✔	✔
Оптимизация Web трафика	Кеширование Web-трафика/ Закачивание файлов большого размера с возможностью предварительного мгновенного сканирования/ Управление трафиком потокового медиа/ Управление входящим и исходящим сетевым трафиком			
Предотвращение утечек данных (DLP функционал)				
Поддержка шаблонов для создания правил безопасности	✔	✔	✔	✔
Поддержка протокола шифрования TLS	✔	✔	✔	✔
Шифрование на уровне сообщений	✔	✔	✔	✔
Словари соответствия	✔	✔	✔	✔
Фильтрация нежелательного контента	✔	✔	✔	✔
Прозрачное восстановление	✔	✔	✔	✔
Сканирование исходящего трафика и контента	✔	✔	✔	✔
Управление исходящими вложениями	✔	✔	✔	✔
Мастер настройки DLP функционала	✔	✔	✔	✔
Классификация исходящих данных	✔	✔	✔	✔
Управление				
Возможности централизованного управления	✔	✔	✔	✔
Создание отчетов отдельно по каждому пользователю	✔	✔	✔	✔
Ведение лог-файлов	✔	✔	✔	✔
Детальная настройка правил безопасности	✔	✔	✔	✔
Детальная настройка отчетов	✔	✔	✔	✔