5NINE SOFTWARE

Защита Microsoft Hyper-V
№1 в мире

Краткое описание

5nine Cloud Security для Hyper-V

Февраль 2014

Microsoft Partner Network

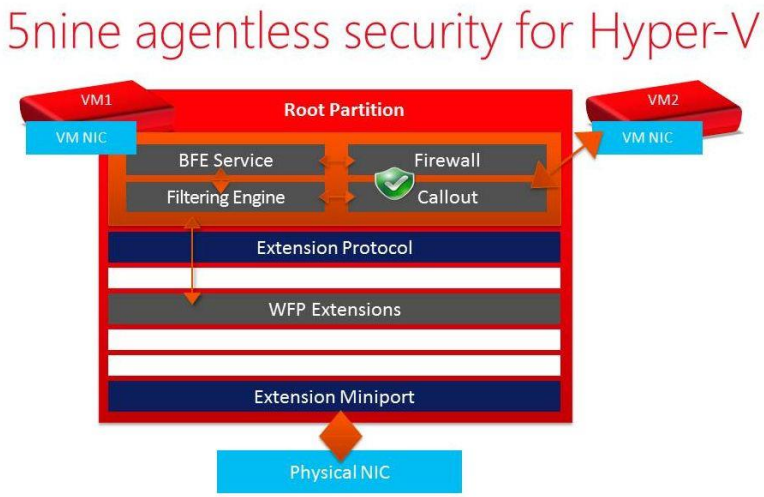
Windows Server 2012 Certified

Windows Server 2012 R2 Certified

Содержание

5nine Cloud Security для Hyper-V

5nine Cloud Security для Hyper-V является первым и единственным безагентным решением для обеспечения безопасности, созданным специально для виртуальной платформы Microsoft: Windows Server 2012/2012R2, Microsoft Hyper-V Server 2012 R2/2012 и Windows 8. Он контролирует сетевой трафик между виртуальными машинами, обнаруживает и блокирует вредоносные атаки, осуществляет быструю антивирусную проверку и повышает безопасность виртуальной среды.



5nine Cloud Security сочетает в себе несколько модулей защиты, в том числе: антивирусный, программируемый межсетевой экран, журнал логов, систему обнаружения вторжений (Intrusion Detection System или IDS), в одном централизованно управляемом программном продукте. Защита Web приложений осуществляется отдельно поставляемым программным продуктом.

Это решение стало возможным с появлением нового интерфейса Windows Filtering Platform (WFP) для Windows 8 и Windows Server 2012/2012R2, новой архитектуры Windows Server Hyper-V Extensible Switch, а также новых мощных API-интерфейсов Microsoft.

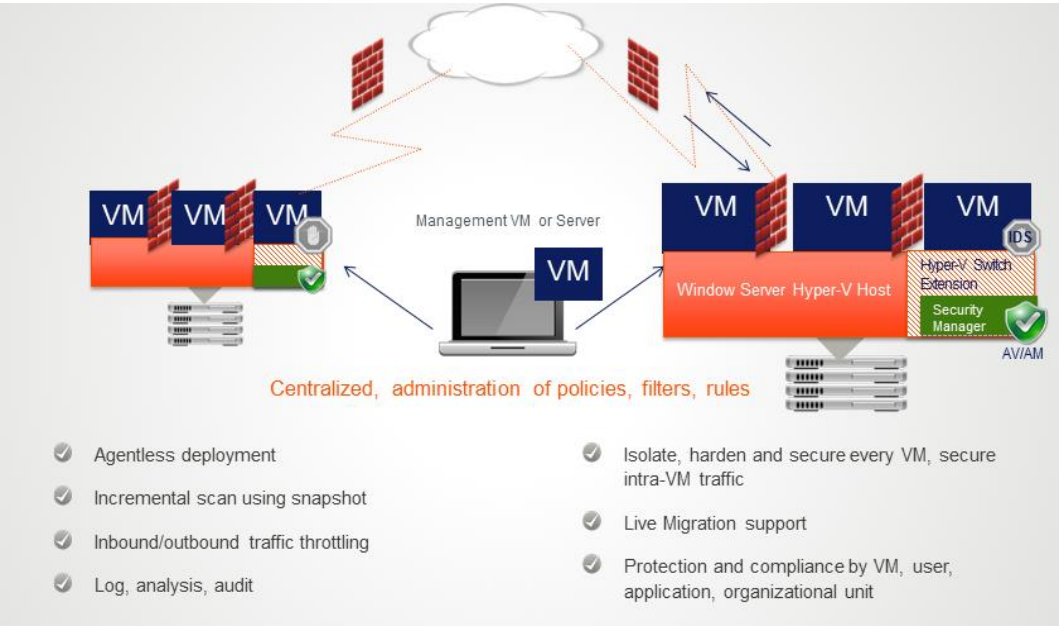
С 5nine Cloud Security предприятия могут:

- Полностью защитить свою виртуальную инфраструктуру в многопользовательском режиме работы с изоляцией виртуальных машин
- Осуществлять быстрое и эффективное антивирусное сканирование виртуальных машин и хостов с использованием уникальных технологий без потери производительности Hyper-V
- Существенно повысить плотность виртуальных машин (ВМ) и эффективность внедрения виртуализации
- Контролировать сетевой трафик между виртуальными машинами
- Обнаруживать и блокировать вредоносные вторжения
- Обеспечить управление с использованием простой и удобной консоли или подключаемого модуля для System Center Virtual Machine Manager (SCVMM)
- Обеспечить соблюдение требований PCI-DSS, HIPAA, Sarbanes–Oxley Act, закона 152-ФЗ «О персональных данных», Приказов № 17 и №21 ФСТЭК и других

5nine Cloud Security соответствует самым жестким и передовым требованиям Security compliance, Best practices in Cloud Security и последним изменениям в российском и зарубежном законодательстве о защите персональных данных в виртуальной среде и соответствия средств защиты информации требованиям регуляторов.

Виртуальный межсетевой экран (Virtual Firewall)

5nine Virtual Firewall контролирует трафик между виртуальными машинами и внешними сетями. Это значительно упрощает развертывание и управление несколькими гостевыми операционными системами, используя расширение нового Hyper-V Extensible Switch.



Виртуальный межсетевой экран в режиме Kernel Mode обеспечивает:

- Фильтрацию MAC-адресов
- ARP правила
- SPI (Stateful Packet Inspection)
- Проверку пакетов и сетевого трафика с анализом аномалий
- Управление входящей и исходящей полосой пропускания с установкой лимитов входящего / исходящего трафика и параметров утилизации для каждой ВМ
- Фильтрацию широковещательного трафика
- Настройку сетевых правил фильтрации для каждой виртуальной машины
- Занесение в журнал всех отфильтрованных событий с расширенным списком данных
- Поддержку режима multi-tenant и возможность создания многопользовательской конфигурации с гибкой ролевой моделью. Теперь владельцы каждого независимого сервиса смогут управлять своими виртуальными машинами в соответствии с правилами, назначенными администратором Hyper-V. При этом как на уровне виртуальной инфраструктуры, так и в каждой ее изолированной части есть возможность создания группы безопасности с правами аудита (просмотра без возможности внесения изменений). А возможность создания изолированной части и назначения группы безопасности и аудита для них осуществляется только администратором Hyper-V
- Создание группы безопасности виртуальных машин, для которых настраиваются единые правила. Например, для настройки обмена трафиком между веб серверами и серверами баз данных возможно создание двух групп и групповых правил вместо индивидуальных для каждой машины. Таким образом, дублируются функции Microsoft Forefront TMG (ISA Server) с поддержкой сетевой виртуализации и решаются основные задачи безопасности, аналогичные TMG для виртуальной среды. Для публикации серверов во

внешнюю сеть по-прежнему используется Microsoft Forefront UAG, возможности которого не пересекаются с решением 5nine и относятся к физической среде

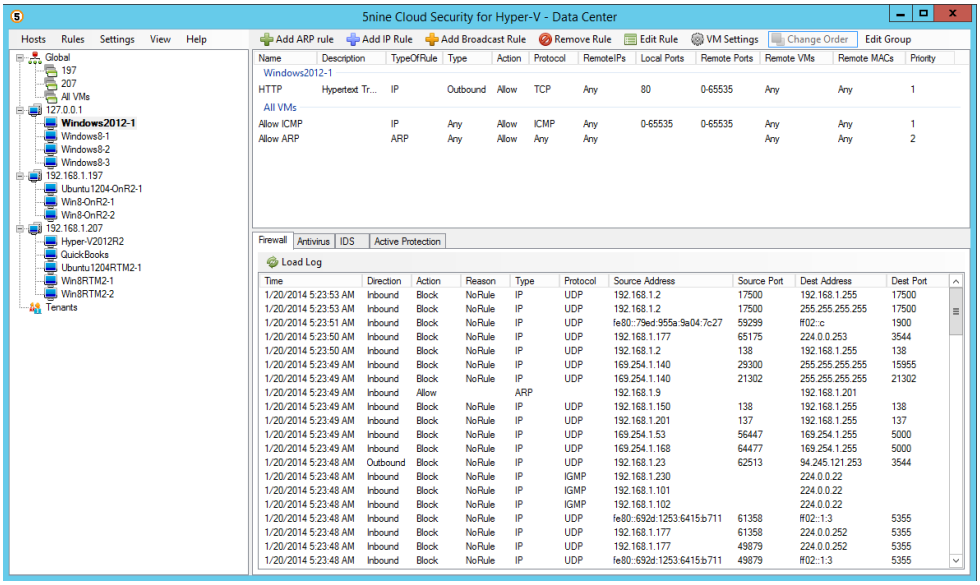
- Применение правил межсетевого экрана и политики фильтрации сети для новых виртуальных машин, которое снижает их уязвимость с момента создания и публикации в виртуальной среде
- Изолирование виртуальных машин и их трафика на одном хосте друг от друга и от интернета, закрыв доступ одних виртуальных машин к другим
- Поддержку механизма сетевой виртуализации NVGRE

Антивирус

В 5nine Cloud Security используется антивирус, который обнаруживает и блокирует вредоносную деятельность и повышает безопасность виртуальной среды Hyper-V без антивирусных «штормов» и снижения производительности, обеспечивая. Антивирус обеспечивает:

- Сохранение производительности с помощью безагентной архитектуры
- Обновление файла сигнатур только на хосте, а не на каждой виртуальной машине
- Поддержку всех видов гостевых операционных систем для Hyper-V
- Быстрое инкрементальное сканирование при помощи CBT драйвера, поблочно отслеживающего изменения в виртуальных дисках VHD/VHDX
- Согласованное управление сканированием с учетом пороговых значений производительности, установленных на виртуальных машинах
- Выборочное сканирование для оптимальной производительности
- Использование антивируса Касперского, адаптированного к среде Hyper-V. Клиенты получают доступ к одной из самых полных и быстро обновляющихся баз сигнатур вирусов в мире и самым передовым технологиям антивирусного сканирования

Централизованная интеллектуальная консоль управления



Интеллектуальная консоль управления 5nine Software централизованно управляет политиками, правилами и фильтрами, избавляя от необходимости изменять и обновлять большое количество агентов и баз данных, обеспечивает контроль безопасности и соответствие

нормам:

- Мощная безагентная архитектура упрощает IT-администрирование
- Централизованная консоль управления обеспечивает простое управление политиками, правилами, фильтрами и журналами
- Все возможности осуществления аудита для обеспечения соответствия нормам

Система обнаружения вторжений (IDS)

5nine Software IDS отслеживает весь трафик внутри виртуального коммутатора Hyper-V, используя технологию Snort для проверки аномалий пакетов, которые могут быть потенциальными атаками или угрозами на уровне приложений:

- Мониторит сетевой трафик и предупреждает о подозрительной активности
- Обеспечивает глубокий уровень защиты приложений

Защита веб-серверов

5nine Web Application Firewall обнаруживает вредоносные действия, в т. ч. DDoS, XSS (Cross-Site Scripting) и другие атаки на веб-сервер. Продукт обнаруживает и блокирует как известные, так и неизвестные типы атак, с подробным анализом данных. 5nine Web Application Firewall могут приобрести только клиенты с IIS веб-серверами.

5nine Web Application Firewall лицензируется на каждый веб-сервер и распространяется по отдельной лицензии.

Поддержка уникальных потребностей хостинг-провайдеров и ЦОД

Требования безопасности для хостинг-провайдеров и ЦОД в виртуальной среде являются очень сложными и гибкими. Виртуальные машины являются уязвимыми для вредоносных программ, вирусов, фишинга и DDoS-атак, а также новых угроз и уязвимостей, не существовавших в физических средах. От распространения вирусов среди виртуальных машин до появления вирусных «штормов» — проблемы в виртуальных средах растут и усложняются.

Традиционные антивирусы, устанавливаемые в виртуальной машине, IDS и межсетевые экраны, созданные для физических сред, не защищают от новых рисков и угроз в виртуализованных средах. Они являются защитой, только если антивирусное ПО установлено на каждой виртуальной машине. В этом случае потребляется ценный ресурс Hyper-V, понижается производительность и увеличиваются IT расходы. Кроме того, ЦОД должен поддерживать бизнес-модель, предусматривающую многопользовательскую безопасность виртуальных машин, клиентов и подразделений для поддержания требуемого уровня качества обслуживания. Безагентная архитектура 5nine Cloud Security обеспечивает бескомпромиссную безопасность, соответствие требованиям и нормам, максимальную производительности для облаков Hyper-V.

Многопользовательский режим безопасности должен поддерживаться для виртуальных машин, клиентов и подразделений, а также обеспечить высокое качество процесса обслуживания клиента во всех деталях. Для обеспечения соответствия нормам, хостинговые компании должны эффективно собирать и проверять данные о каждой виртуальной машине, контролировать и защищать трафик внутри виртуальной машины.

С 5nine Cloud Security для Hyper-V хостинг-провайдеры и ЦОД могут:

- Повысить производительность платформы, плотность виртуальных машин и окупаемость проекта за счет использования расширения Hyper-V Extensible Switch
- Упростить развертывание средств безопасности
- Предотвратить «антивирусные штормы»
- Поддерживать многопользовательскую среду с полной защитой Public Cloud и разделением ролей администраторов IT, безопасности и аудитора
- Обеспечить безопасность и соответствие требованиям Федерального закона 152-ФЗ "О персональных данных" для виртуальной инфраструктуры и иметь возможность размещать у себя в ЦОД клиентов с повышенными требованиями к безопасности на основе выполнения требований к средствам защиты информации в виртуальной среде
- Продавать услуги, соответствующие требованиям 152-ФЗ в виртуальной среде
- Предоставить клиентам дополнительные услуги, такие как безагентный антивирус и управление безопасностью виртуальной машины
- Обеспечить низкую цену построения системы безопасности ЦОД и конкурентные цены на услуги защиты виртуальных машин для клиентов

Информация для заказа продуктов и поддержки

- http://www.5nine.ru
- E-mail: info@5nine.ru
- Тел.: +7 (495) 777-32-82