ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

Модуль Cisco Catalyst WS-SVC-FWM-1-K9

WS-SVC-FWM-1-K9

Описание

• Производительность 5.5G на модуль

• до 4 модулей (20G) на шасси Catalyst 6500

• Пропускная способность - 2.8 Мп/с

• 1M соединений

• скорость установки 100 000 соединений в секунду

• 256,000 NAT/PAT трансляций

• поддержка Jumbo Ethernet packets (8500)

Модуль сервисов межсетевого экрана для серии Cisco Catalyst 6500 (Cisco Catalyst 6500 Series Firewall Services Module, FWSM)– это высокоскоростной, интегрированный модуль межсетевого экрана для коммутаторов серии Cisco Catalyst 6500 и маршрутизаторов серии Cisco 7600, который обеспечивает пропускную способность 5,5 Гб/сек., скорость установления соединений 100 000 в секунду и 1 миллион одновременных соединений. На одном шасси можно установить до 4 модулей FWSM, с масштабируемостью вплоть до 20 Гб/сек на каждое шасси. FWSM входит в семейство устройств обеспечения безопасности Cisco PIX и гарантирует крупным компаниям и провайдерам услуг безопасность, надежность и производительность самого высокого уровня. В модулях FWSM применяется технология Cisco PIX и работает действующая в режиме реального времени, надежная встроенная ОС Cisco PIX, которая устраняет ”дыры” в системе защиты, негативно отражающиеся на производительности. Центральное звено системы – это схема защиты, основанная на адаптивном алгоритме защиты (Adaptive Security Algorithm, ASA), которая выполняет функции межсетевого экрана, ориентированные на учет статуса соединений. Используя ASA, FWSM создает запись таблицы соединений для сеансового потока трафика на основании адресов отправителя и получателя, выбираемых по случайному принципу порядковых номеров сегментов TCP, номеров портов и дополнительных флагов TCP. FWSM контролирует

весь входящий и исходящий трафик, применяя политику безопасности к этим записям таблицы соединений.

В FWSM реализован ряд функций высокого уровня, включая множественные контексты безопасности на маршрутизируемых уровнях и в режиме моста (bridging mode). Это помогает снизить расходы и сложность операций и при этом обеспечить управление несколькими межсетевыми экранами с одной управленческой платформы. Виртуализация на FWSM создает дополнительную защиту инвестиций, эффективность которых уже гарантирована применением коммутаторов серии Cisco Catalyst 6500 и маршрутизаторов серии 7600. Виртуализация FWSM в сочетании с другими сервисами обеспечения безопасности, которые заложены в коммутаторах серии Cisco Catalyst 6500 и в маршрутизаторах серии Cisco 7600, - это мощное решение по созданию глубокой системы защиты. Используя такие функции, как, например, менеджер ресурсов (Resource Manager), компании могут ограничить ресурсы, выделяемые в любой конкретный момент времени на любой контекст обеспечения безопасности. Благодаря этому не возникает конфликта контекстов безопасности. При наличии стандартной лицензии на программное обеспечение возможна работа двух контекстов обеспечения безопасности в дополнение к специальному административному контексту. Для использования большего количества контекстов безопасности требуется приобрести лицензию.

При использовании функции прозрачного межсетевого экрана, которая настраивает FWSM для работы в качестве межсетевого экрана уровня 2 (Layer 2 bridging firewall), необходимы лишь минимальные изменения в сетевой топологии. Использование прозрачного межсетевого экрана (transparent firewall) сокращает как время конфигурирования, так и время развертывания – это несомненный плюс для любого бизнеса, располагающего ограниченными ресурсами в области ИТ. Здесь нет IP-адресов кроме как для интерфейса управления. При использовании прозрачных межсетевых экранов не требуется дополнительное разбиение на сети на подсети и изменение ее конфигурации.

Функции управления сервисами FWSM обеспечивают более эффективное предоставление и мониторинг сервисов безопасности, даже в рамках и с охватом нескольких виртуальных контекстов. Сюда входит создание классов, ограничение ресурсов, списки контроля доступа (ACL), индивидуальные для каждого пользователя/на базе сервера управления доступом Cisco Access Control Server (ACS), системные журналы для каждого ACL, конфигурация на уровне системных журналов, инспектирование протокола Address Resolution Protocol (ARP) и поддержка пересылки многоадресных пакетов (multicast pass-through).

Усовершенствованная фильтрация обеспечивает дополнительную защиту и поддержку приложений, в частности голосовых приложений. Кроме этого, предусмотрены основанная на правилах политики трансляция сетевых адресов (Network Address Translation, NAT), двунаправленная NAT, двунаправленные фильтры, поддержка IP-телефонии (VoIP), трансляция адресов портов (Port Address Translation, PAT) для протокола Skinny и протокола SIP (Session Initiation Protocol), протокол взаимодействия между программой управления соединениями и шлюзами (Gateway Control Protocol, MGCP), H.323 v3 и v4. А также многопротокольная коммутация на основе меток (Multiprotocol Label Switching, MPLS) и интеграция межсетевого экрана, фильтрация URL с применением WebSense и N2H2, блокирование атак.

Основные особенности.

Интегрированный модуль
FWSM, установленный в коммутаторе Cisco Catalyst серии 6500 или маршрутизаторе Cisco серии 7600, дает любому порту коммутатора возможность выполнять функции порта межсетевого экрана, а также интегрирует в сетевую инфраструктуру функции безопасности межсетевого экрана, действующие с учетом параметров состояния. Это играет особенно важную роль, если основополагающим фактором выступает пространство стойки. Коммутаторы Cisco Catalyst серии 6500 и маршрутизаторы Cisco серии 7600 фактически становятся оптимальными коммутаторами с сервисами IP для тех клиентов, которым требуются интеллектуальные сервисы, в частности, сервисы межсетевого экрана, выявления вторжений и ресурсы VPN, наряду с многоуровневыми территориальными, локальными и городскими сетями.

Готовность к будущему
Модуль FWSM может обрабатывать трафик с интенсивностью до 5 Гб/сек., обеспечивая отличное быстродействие для удовлетворения будущих требований без необходимости капитальной перестройки системы. Для удовлетворения растущих требований к серии Cisco Catalyst 6500 можно добавить до трех

ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

дополнительных модулей FWSM, т.е. использовать в общей сложности четыре модуля.
Надежность и высокая готовность
FWSM создан на базе технологии Cisco PIX, в нем применяется надежная, апробированная, работающая в реальном времени операционная система Cisco PIX. Модуль FWSM – это уникальное сочетание быстродействия и надежности на одной платформе с использованием апробированной технологии Cisco PIX для инспектирования пакетов. Для обеспечения устойчивой работы модуль FWSM поддерживает высокоскоростной перехват функций управления в случае сбоя между модулями на одном шасси 6500 или 7600 и между модулями на отдельных шасси. Такая поддержка восстановления работоспособности после возникновения сбоев дает клиентам полную свободу действий в развертывании межсетевых экранов.
Менее высокая стоимость владения
Модуль FWSM – это оптимальное сочетание цены и эффективности работы межсетевого экрана. Поскольку основой модуля FWSM служит межсетевой экран Cisco PIX, снижаются затраты на обучение и управление; поскольку модуль FWSM интегрирован в шасси, уменьшается количество управляемых устройств.

Простота управления
Интуитивный графический пользовательский интерфейс программы-менеджера устройств Cisco PIX (Cisco PIX Device Manager) можно использовать для управления и конфигурации функций в FWSM. Модуль FWSM поддерживается инфраструктурой управления Cisco, и партнерами AVVID (Architecture for Voice, Video and Integrated Data) по настройке и мониторингу. Cisco PIX Device Manager обеспечивает возможность упрощенного управления и мониторинга FWSM на уровне системы и устройства, а также большей детализации на уровне контекста безопасности.

Характеристики.

Производительность	5.5 Гб/сек 1 миллион одновременных соединений Установление и разрыв 100 000 соединений в секунду 256 000 PAT и 256 000 NAT трансляций
Маршрутизируемый и прозрачный межсетевой экран	Межсетевой экран может работать в одном из следующих режимов: Маршрутизируемый (Routed) - Модуль FWSM рассматривается как маршрутизатор в сети. Прозрачный (Transparent) - Модуль FWSM действует как “узелок на проводе” и не является точкой маршрутизации. Модуль FWSM соединяет одну и ту же сеть на ее внутренних и внешних портах, но при этом необходимо, чтобы каждый порт находился в другой VLAN. Протоколы динамической маршрутизации и NAT отсутствуют.
Режим виртуального межсетевого экрана (несколько контекстов безопасности)	В режиме виртуального межсетевого экрана вы можете создать до ста отдельных контекстов безопасности (в зависимости от имеющейся у вас лицензии на программное обеспечение). Контекст безопасности – это виртуальный межсетевой экран, имеющий собственную политику безопасности и интерфейсы. Каждый виртуальный межсетевой экран может поддерживать 256 сетей VLAN в маршрутизируемом режиме. Прозрачный режим поддерживает только два интерфейса на контекст. Несколько контекстов – это аналог наличия нескольких автономных межсетевых экранов. Все контексты безопасности могут действовать в маршрутизируемом режиме или в прозрачном режиме.
Двунаправленная NAT и NAT на базе	Динамическая/статическая NAT и PAT. Вы можете конфигурировать NAT на внутренних и внешних адресах. Для NAT на

ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

NAT и NAT на базе политики	Вы можете конфигурировать NAT на внутренних и внешних адресах. Для NAT на базе политики вы можете идентифицировать адреса, которые будут транслироваться с использованием расширенного ACL. Это даст вам дополнительный контроль над отбором адресов для трансляции.
Управление ресурсами	ООграничение ресурсов, выделяемых на каждый контекст, таким образом, чтобы ни один контекст не расходовал все доступные ресурсы.
Коммуникация ресурсов с одинаковым уровнем безопасности	Возможность коммуникации интерфейсов, у которых одинаковый уровень безопасности, без NAT/статических политик. Возможность вводить ограничение максимального количества соединений индивидуально для хостов.
Фильтрация URL	Фильтрация запросов HTTP, HTTPS и FTP с использованием механизмов фильтрации WebSense Enterprise или фильтрации HTTP в N2H2 (сегодня входит в Secure Computing Corporation).
Поддержка конфигурации	Консоль к интерфейсу командной строки (CLI) Telnet к внутреннему интерфейсу модуля FWSM. Telnet через IPSec к внешнему интерфейсу модуля FWSM. Протокол SSH к CLI. Протокол SSL к менеджеру устройств Cisco PIX Device Manager. Центр управления CiscoWorks VMS Management Center for Firewalls.
Поддержка AAA	Интеграция с популярными сервисами аутентификации, авторизации и аудита (AAA) через поддержку TACACS+ и RADIUS.
Cisco PIX Device Manager	Простой и интуитивный графический вэб-интерфейс пользователя поддерживает удаленное управление межсетевыми экранами. Различные отчеты – в реальном времени и статистические – предоставляют информацию о тенденциях, базовых характеристиках эффективности и событиях, связанных с безопасностью. Кроме этого, Cisco PIX Device Manager интегрирован в комплексный инструмент управления устройствами, предназначенный для линейки Cisco Catalyst 6500 - менеджер устройств CiscoView Device Manager. Из CiscoView Device Manager можно осуществлять коллективное управление модулями, входящими в систему Cisco Catalyst 6500, в частности, модулем FWSM и модулем надзора, используя простой графический пользовательский интерфейс.
Надежное управление сетями	Использование 3DES – защищенный доступ к управлению сетями.
Списки доступа (ACL)	Вплоть до 80 000 списков ACL. Поддерживаются списки ACL следующих типов: Расширенный ACL для контроля IP-трафика на интерфейсе: Входящий. Исходящий.

	исходящий. Для режима прозрачного межсетевого экрана - EtherType ACL для контроля не IP-трафика на интерфейсе: Входящий. Исходящий. Стандартный ACL для перераспределения маршрутов по протоколу предпочтения кратчайшего пути OSPF (Open Shortest Path First). Индивидуальные для каждого пользователя списки ACL с использованием Cisco Secure ACS.
Протоколы динамической маршрутизации	В одноконтекстном режиме модуль FWSM поддерживает следующие протоколы маршрутизации: Протокол маршрутизации Routing Information Protocol (RIP) v1 и v2 (пассивный режим) Протокол OSPF. В прозрачном режиме поддерживается только статическая маршрутизация.
Авторизация команд	Дает вам возможность контролировать доступ пользователей к командам и создавать пользовательские учетные записи или логины, привязанные к уровням привилегий.
Группировка объектов	Возможность группировать сетевые объекты (например, хосты) и сервисы (FTP и HTTP) для списков ACL.
Защита от атак типа отказ в обслуживании (DoS)	Защита системы доменных имен DNS Guard. Защита от перегрузки ресурсов Flood Defender. Защита от перегрузки ресурсов Flood Guard. Перехват TCP с оптимизацией SYN cookies (TCP Intercept with SYN cookies optimization). Однонаправленная проверка передачи по обратному пути (Unicast Reverse Path Forwarding, uRPF). Защита почты Mail Guard. FragGuard и Virtual Reassembly. Инспектирование с учетом параметров состояния по протоколу ICMP (Internet Control Message Protocol). Контроль интенсивности по протоколу UDP.
Инспектирование ARP	В режиме прозрачного межсетевого экрана модуль FWSM сопоставляет MAC-адрес и IP-адрес во всех пакетах ARP со статическими записями в таблице ARP.
Протокол DHCP	Модуль FWSM действует как сервер DHCP. Кроме этого, модуль FWSM поддерживает ретрансляцию DHCP для пересылки запросов DHCP на вышестоящий маршрутизатор.

ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

Высокая готовность	Переключение на резервный модуль с учетом параметров состояния и без разрыва текущих соединений как внутри шасси так и между шасси.
Регистрация	Комплексная системная регистрация, регистрация FTP, URL и ACL регистрация.
Дополнительные протоколы	H.323 v3 и 4. NetBios over IP. RAS, версия 2. Real-Time Streaming Protocol (RTSP). SIP с PAT. XDMCP. Skinny.

Общие

Тип устройства	Сервисный модуль
Линейка Cisco	Catalyst 6500, 6500-E
Производительность модульного коммутатора, Gbps	5,5
Совместимая платформа	Шасси WS-C6506 Шасси WS-C6509 Шасси WS-C6513 Шасси WS-C6503
Совместимость с управляющими модулями	WS-SUP720-3BXL WS-SUP720-3B VS-S720-10G-3C VS-S720-10G-3CXL VS-S2T-10G VS-S2T-10G-XL