Содержание

Введение

Этот документ описывает, как разработать Cisco Web Security Appliance (WSA) и привязанные компоненты для оптимальной производительности.

Общие сведения

При разработке решения для WSA это требует должного внимания, не только в отношении конфигурации самого устройства, но также и связанных сетевых устройств и их функций. Каждая сеть является совместной работой составных устройств, и если один из них не участвует правильно в сети, то пользовательский опыт мог бы уменьшиться.

Существует два основных компонента, которые нужно рассмотреть, когда вы настраиваете WSA: аппаратные средства и программное обеспечение. Аппаратные средства прибывают в два различных типа. Первым является физический тип аппаратных средств, таких как S170, S380, и Модели серии S680, а также другой конец Жизни (EoL) модели, такие как S160, S360, S660, S370 и Модели серии S670. Другой тип оборудования является действительным, таким как S000v, S100v и Модели серии S300v. Операционную систему (OS), которая работает на этих аппаратных средствах, называют *AsyncOS для сети*, которая основывается на FreeBSD в его ядре.

WSA предлагает сервис proxy и также просматривает, осматривает и категоризирует весь трафик (HTTP, HTTPS и Протокол FTP). Все эти протоколы, выполненные поверх TCP и в большой степени, полагаются на Систему доменных имен (DNS) для правильной работы. По этим причинам исправность сети жизненно важна для правильной работы устройства и его связи с различными частями сети, и внутри и снаружи контроля предприятия.

Дизайн

Используйте информацию, которая описана в этом разделе для разработки WSA и отнесенных компонентов для оптимальной производительности.

Сеть

Безошибочная, быстрая сеть жизненно важна для правильной работы WSA. Если сеть нестабильна, пользовательский опыт мог бы уменьшиться. Когда веб-страницы занимают больше времени для достижения или недостижимы, проблемы сети обычно обнаруживаются. Начальный наклон является виной устройство, но это обычно - сеть, которая плохо себя ведет. Таким образом должное внимание и аудит должны быть сделаны, чтобы гарантировать, что сеть предлагает лучшую услугу для высокоуровневых прикладных протоколов, таких как HTTP, HTTPS, FTP и DNS.

Общие рекомендации

Вот некоторые общие рекомендации, которые можно внедрить для обеспечения лучшего поведения сети:

- Гарантируйте, что сеть (L2) Уровня 2 стабильна, что операция связующего дерева корректна, и что нет частых вычислений связующего дерева и изменений топологии.
- Протокол маршрутизации, который используется, должен также предоставить быструю конвергенцию и устойчивость. Протокол OSPF быстрые таймеры или Протокол EIGRP является хорошими выборами для такой сети.
- Всегда используйте по крайней мере два интерфейса данных на WSA: тот, который стоит перед компьютерами конечного пользователя и другим для исходящей операции (связанный с прокси восходящего канала или Интернетом). Это сделано для устранения возможного ресурса, ограничивает, такой как тогда, когда количество портов TCP исчерпано или когда сетевые буферы становятся полными (с использованием одни интерфейсы для и внутри и снаружи особенно).
- Выделите Интерфейс управления для трафика толька для управления для увеличения безопасности. Для достижения этого через GUI перейдите к **Сети> Интерфейсы** и проверьте **Отдельную маршрутизацию (порт M1, ограниченный только сервисами управления устройства)** флажок.
- Используйте быстрые серверы DNS. Любая транзакция через WSA требует по крайней мере одного Поиска DNS (если не в кэше). Сервер DNS, который является медленным или плохо себя ведет, влияет на любую транзакцию и наблюдается, как задержано или медленное интернет-соединение.
- Когда таблицы отдельной маршрутизации используются, эти правила применяются:

  Все интерфейсы включены в таблицу маршрутизации *менеджмента* по умолчанию (M1, P1, P2).

Только Интерфейсы данных включены в таблицу *Маршрутизации данных*.

Примечание: Разделение таблиц маршрутизации не для интерфейса, а скорее для сервиса. Например, трафик между WSA и Microsoft Active Directory (AD), контроллер домена всегда повинуется маршрутам, которые заданы в таблице маршрутизации менеджмента, и возможно настроить маршруты, которые указывают из интерфейса P1/P2 в этой таблице. Не возможно включать маршруты в таблицу Маршрутизации данных, которые используют Интерфейсы управления.

Распределение нагрузки

Вот некоторые распределяющие нагрузку факторы, которые можно внедрить для обеспечения лучшего поведения сети:

- Вращение DNS? Это - термин, использованный, когда одиночное имя хоста используется в качестве прокси, но это имеет множественный записи на сервере DNS. Каждый клиент решает это к другому IP-адресу и использует другие прокси. Ограничение - то, что изменения записей DNS отражены на клиентах на перезагрузку (кэширование локального DNS), таким образом, это предлагает нижний уровень устойчивости, если должно быть внесено изменение. Однако это прозрачно конечным пользователям.

- Файлы Контроля за прокси - адресом (PAC)? Это файлы сценариев прокси автоматические, которые определяют, как каждый URL должен быть обработан на браузере на основе записанных функций в нем. Это имеет функцию для передачи того же URL всегда непосредственно или к тому же прокси.

- Автоматическое обнаружение? Это описывает использование методов DNS/DHCP для получения файлов PAC (описанный в предыдущем рассмотрении). Обычно, эти первые три факторов объединены в одно решение. Однако это может быть сложно и много user-agent, таких как Microsoft Office, Adobe Downloader, Javascripts и Флэш, не могут считать файлы PAC вообще.

- Протокол управления веб-кэша (WCCP)? Этот протокол (особенно Версия 2 wccp) предоставляет устойчивое и очень действенный способ, чтобы создать распределение нагрузки между несколькими WSAs и также включить высокую доступность.

- Отдельное устройство (устройства) распределения нагрузки? Cisco рекомендует использовать балансировщики загрузки в качестве специализированных машин.

Межсетевые экраны

Вот некоторые факторы Межсетевого экрана, которые можно внедрить для обеспечения лучшего поведения сети:

- Гарантируйте, что Протокол ICMP позволен всюду по сети из каждого источника. Это жизненно важно, поскольку WSA зависит от пути механизм обнаружения Maximum Transition Unit (MTU), как описано в RFC 1191, который зависит от Эхо-запросов

протокола ICMP (тип 8) и Эхо - ответы (тип 0), и фрагментация сообщения о недоступности ICMP требуется (тип 3, код 4). Если вы отключаете обнаружение MTU-маршрута на WSA с **pathmtudiscovery** командой CLI, то WSA использует MTU по умолчанию 576 байтов согласно RFC 879. Это влияет на производительность в связи с к увеличенным издержкам и повторной сборке пакетов.

- Гарантируйте, что нет никакой асимметричной маршрутизации в сети. В то время как это не проблема на WSA, любой Межсетевой экран, с которым встречаются вдоль пути, отбрасывает пакеты, потому что это не получило обе стороны связи.

- С Межсетевыми экранами очень важно исключить IP-адреса WSA из угроз как обычные конечные компьютерные станции. Межсетевой экран мог бы поместить в черный список IP-адреса WSA из-за слишком многих соединений (согласно общему знанию Межсетевого экрана).

- Если Технология NAT используется для какого-либо IP-адреса WSA на устройстве абонентского оборудования, гарантируйте, что каждый WSA использует отдельный внешний глобальный адрес в NAT. При использовании NAT для множественных WSAs, которые имеют одиночный внешний глобальный адрес, вы могли бы встретиться с этими проблемами:

  Все соединения от всех WSAs к внешнему миру используют одиночный внешний глобальный адрес, и Межсетевой экран быстро исчерпывает ресурсы.

  Если существует скачок трафика к тому одному месту назначения, сервер назначения мог бы поместить в черный список его и отключить все предприятие от доступа до этого ресурса. Это могло бы быть ценным ресурсом как компанией "Облачное" хранилище, Облачные соединения офиса или обновления антивирусного программного обеспечения на компьютер.

Личности

Помните, что *логический* принцип *AND* применяется во всех составляющих идентичности. Например, при настройке и user-agent и IP-адреса это означает user-agent *от* этого IP-адреса. Это не означает user-agent *или* этот IP-адрес.

Используйте одну идентичность для аутентификации того же суррогатного типа (или никакой заместитель) и/или user-agent.

Важно гарантировать каждую идентичность, которая требует, чтобы аутентификация включала строки user-agent для известных браузеров/user-agent, которые поддерживают проверку подлинности прокси-сервера, такую как Internet Explorer, Mozilla Firefox и Google Chrome. Существуют некоторые приложения, которые требуют доступа в Интернет, но не поддерживают аутентификацию прокси/WWW.

С личностями совпадают от начала до конца с поиском соответствий, который заканчивается на первой записи, с которой совпадают. Поэтому, если у вас есть *Идентичность 1* и *Идентичность 2* настроенных, и транзакция совпадает с Идентичностью 1, это не проверено против Идентичности 2.

Политика Вредоносного ПО доступа/Расшифровки/Маршрутизации/Исходящего

Эта политика применена против различных типов трафика:

- Политика доступа применена против простого HTTP или FTP - соединений. Они определяют, должна ли транзакция быть принята или отброшена.

- Политика расшифровки определяет, должны ли транзакции HTTPS быть дешифрованы, отброшены или пройтись. Если транзакция дешифрована, то последовательная часть ее может быть замечена как простой запрос HTTP и совпадается против Политики доступа. Если необходимо отбросить Запрос HTTPS, отбросить его в Политике расшифровки, не в Политике доступа. В противном случае это использует больше ЦП и памяти для отброшенной транзакции сначала, чтобы быть дешифрованным и затем быть отброшенным.

- Политика маршрутизации определяет восходящее направление транзакции однажды это его позволенный через WSA. Это применяется, если существуют прокси восходящего канала или если WSA находится в режиме *Разъёма* и передает трафик к Облачной веб-башне Безопасности.

- Исходящая вредоносная политика применена против HTTP или загрузок FTP от конечных пользователей к Web-серверам. Это обычно замечается, запрос Поста HTTP.

Для каждого типа политики важно помнить, что применяется *логический* принцип *OR*. Если вам обратились множественные личности, то транзакция должна совпасть с любой из личностей, которые настроены.

Для более тонкой настройки используйте эту политику. Неправильно настроенные личности на политику могут создать проблемы, где это более выгодно для использования нескольких личностей, на которые ссылаются в политике. Помните, что личности не влияют на трафик, они просто определяют типы трафика для более поздних соответствий в политике.

Часто времена, Политика расшифровки использует личности с аутентификацией. В то время как это не неправильно и иногда необходимо, использование идентичности с аутентификацией, на которую ссылаются в Политике расшифровки, означает, что все транзакции, которые совпадают с Политикой расшифровки, дешифрованы для аутентификации для имения место. Действие расшифровки могло бы быть отброшено или пройтись, но так как существует идентичность с аутентификацией, расшифровка имеет место, чтобы позже понизиться или пройти через трафик. Это дорого и должно избежаться.

Некоторые конфигурации наблюдались, которые содержат 30 или больше личностей и 30 или больше Политики доступа, где вся Политика доступа включает все личности. В этом случае нет никакой потребности использовать это много личностей, если с ними совпадают во всей Политике доступа. В то время как это не вредит операции устройства, она создает беспорядок с попытками устранить неполадки и дорога в отношении производительности.

Пользовательские категории URL

Использование пользовательских категорий URL является мощным программным

средством на WSA, который обычно неправильно понимается и неправильно используется. Например, существуют конфигурации, которые содержат все видео-сайты для соответствий в идентичности. WSA имеет встроенное программное средство, которое автоматически обновляет, когда видео-сайты изменяют URL, который часто происходит. Таким образом это целесообразно позволять WSA управлять категориями URL автоматически и использовать пользовательские категории URL для специального предложения, еще категоризированные узлы.

Будьте очень осторожны с регулярными выражениями. Если соответствия специального символа, такие как точка (.) и звезда (*) используются, они, могло бы оказаться, были бы очень ЦП и обширной памятью. WSA разворачивает любое регулярное выражение для соответствия с ним против каждой транзакции. Например, вот регулярное выражение:

Это выражение будет совпадать с любым URL, который содержит *пример* слова, не только *example.com* домен. Избегите использования *точки* и *звезды* в регулярных выражениях и используйте их только как последнее прибежище.

Вот другой пример регулярного выражения, которое могло бы создать проблемы:

При использовании данного примера в поданных Регулярных выражениях он будет не только совпадать *с www. пример. com*, но также и *www www3example2com.com*, поскольку точка здесь означает *любой символ*. Если вы желаете совпасть только *с www. пример. com*, выйдите из точки:

В этом случае, когда можно включать эту внутреннюю часть пользовательский домен категории URL с этим форматом, нет никакой причины использовать функцию Регулярных выражений:

Антивирус и репутация

Если несколько механизмов сканирования включены, полагайте, что опция включает адаптивное сканирование также. Адаптивное сканирование является мощным, но маленьким механизмом на WSA, который предварительно просматривает каждый запрос и определяет всесторонний механизм, который должен использоваться для сканирования запросов. Это немного увеличивает производительность на WSA.