VPN ASA, балансирующая нагрузку основного процесса голосования

Содержание

Введение

Этот документ описывает Основной Процесс голосования в сценарии распределения нагрузки VPN с Устройством адаптивной защиты (ASA) Cisco 5500-X Series.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco ASA, 5500-X, который работает под управлением ПО версии 9.2.

> **Примечание:** Этот документ также применяется ко всем версиям программного обеспечения, так как функция была сначала представлена в Версии 7.0 (1).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Распределение нагрузки VPN является механизмом, который используется для равноправного распределения сетевого трафика среди устройств в виртуальном кластере. Распределение нагрузки основывается на простом распределении; это не принимает для учета использования пропускной способности или других факторов. Распределяющий нагрузку кластер состоит из двух или больше устройств, ведущего устройства и одного или более дополнительных устройств, и эти устройства не должны быть настроены тождественно.

Распределение нагрузки алгоритма

Вот обзор распределяющего нагрузку алгоритма:

- Ведущее устройство поддерживает сортированный список вторичных членов кластера в порядке возрастания внутренних IP-адресов.
- Загрузка вычислена как целочисленный процент (количество активных / максимальных пропускных способностей для сеанса), который предоставлен каждым вторичным членом кластера.
- Ведущее устройство перенаправляет IPSEC/УРОВЕНЬ ЗАЩИЩЕННЫХ СОКЕТОВ (SSL) VPN-туннель к устройству с самой низкой загрузкой сначала, пока это не на один процент выше, чем другие устройства.
- Ведущее устройство перенаправляет к себе только, когда все вторичные члены кластера на один процент выше, чем ведущее устройство.

Вот пример с одним ведущим устройством и двумя вторичными членами кластера:

- Все узлы начинаются с загрузки нулевого процента, и все проценты округлены к самому близкому полупроценту.
- Ведущее устройство берет соединение, если у всех участников есть загрузка, которая на один процент выше, чем ведущее устройство.
- Если ведущее устройство не берет соединение, сеанс взят устройством резервного копирования, которое в настоящее время имеет самый маленький процент загрузки.
- Если у всех участников есть тот же процент загрузки, то устройство резервного копирования с наименьшим количеством суммы сеансов берет сеанс.
- Если у всех участников есть тот же процент загрузки и то же количество сеансов, то

устройство резервного копирования с наименьшим количеством суммы IP-адресов берет сеанс.

Основной процесс голосования

VPN, балансирующая нагрузку Основного Процесса голосования, выполнена на кластерной внешней сети. Существует два типа данных, переданных на внешней сети:

- Обмениваются пакетами Протокола ARP для кластерного IP-адреса, которые используются для основного обнаружения. Максимальное число пакетов ARP, которые передаются за кластерным IP-адресом для обнаружения ведущего устройства:

  (10 - приоритет) + 1

  Здесь, *приоритет* настроен как в **приоритетной** подкоманде команды CLI **распределения нагрузки vpn**.

- Пакетами UDP на внешней стороне для запроса/ответных сообщений Hello обмениваются. Номер порта задан в **кластерной** подкоманде распределения нагрузки **порта** и является по умолчанию к **9023**.

Как пример, если *приоритет* пять для распределяющего нагрузку устройства, он пытается передать до шести пакетов ARP, чтобы видеть, владеет ли какое-либо ведущее устройство кластерным IP-адресом. Если ведущее устройство обнаружено, ASA больше не передает сообщения ARP и ждет за 15 секунд до того, как это отправит UDP запрос Hello. Ведущее устройство тогда отвечает UDP ответ Hello.

Предупреждение для сценариев перезагрузки

В ситуации с перезагрузкой с двумя ASA в распределяющем нагрузку кластере:

- Или ASA 1 или ASA 2 были ведущим устройством перед перезагрузкой.
- ASA 1 перезагружен.
- ASA 2 становится ведущим устройством, если это не было ведущее устройство ранее.
- ASA 1 просто присоединяется к кластеру как ведомое устройство после перезагрузки.

На распределяющий нагрузку алгоритм могла бы влиять конфигурация коммутатора, где внешний интерфейс кластерных устройств связан также. Например, Алгоритм связующего дерева мог бы вызвать задержку связи, когда перезагружено устройство, которое связано с коммутатором.

Совет: Порт связующего дерева быстрая команда помогает ускорять процесс.

В некоторых случаях недавно перезагруженный ASA, который имеет распределение нагрузки, включил, мог бы попытаться стать ведущим устройством (даже если ведущее устройство уже существует) , потому что это не может достигнуть текущего ведущего

устройства из-за задержки связи в коммутаторе. Когда существует конфликт мастерства, обнаруженный в результате коллизии ARP, ASA с низким Адресом для управления доступом к среде (MAC) побеждает, в то время как ASA с более высоким MAC-адресом бросает роль ведущего устройства.

Основной процесс переизбрания

Существует две ситуации, которые вызывают переизбрание ведущего устройства.

Ведущее устройство, удаленное из кластера

Когда вы отключаете опцию на ASA, широковещательное сообщение передается всем членам кластера для информирования об изменении, и ранее описанный процесс голосования выполнен.

Ведущее устройство Не Отвечает на Приветственные сообщения Члена кластера

Если ведущее устройство не отвечает на Приветственное сообщение члена кластера, члену кластера ASA требуются приблизительно 20 секунд, чтобы обнаружить, что больше не присутствует ведущее устройство. Приветственные сообщения передаются каждые пять секунд (не конфигурируемые). Если члены кластера не получают ответ от ведущего устройства после четырех Приветственных сообщений, то процесс голосования инициирован.

Устранение неполадок

> **Примечание:** См. статью Important Information on Debug Commands Cisco перед использованием **команд отладки**.

Эти команды отладки могут быть полезными с попытками решить проблемы с вашей системой:

- **fsm 255 отладки** - Использование эта команда для активации общей отладки Блока конечных состояний. Введите **команду no debug all** для деактивации.
- **меню vpnlb 3 отладки** - Использование эта команда для активации VPN, балансирующей нагрузку трассировки отладки. Введите **команду vpnlb 3 меню отладки** еще раз для деактивации.
- **меню vpnlb 4 отладки** - Использование эта команда для активации распределения нагрузки VPN функционирует трассировка. Введите **команду vpnlb 4 меню отладки** еще раз для деактивации.

Дополнительные сведения

- Понимание распределения нагрузки
- Cisco Systems – техническая поддержка и документация