Пример конфигурации балансировки нагрузки удаленного клиента VPN Client на ASA 5500

Содержание

Введение

Выравнивание нагрузки позволяет совместно использовать VPN-клиент Cisco с несколькими модулями устройства адаптивной защиты (ASA) без вмешательства пользователя. Распределение нагрузки гарантирует, что публичный IP-адрес будет доступен пользователям с высокой степенью уверенности.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Вы имеете назначенные IP - адреса на своих ASA и настроили шлюз по умолчанию.
- IPsec настроен на ASA для Пользователей VPN-клиента.
- Пользователи VPN в состоянии подключить со всеми ASA с использованием их индивидуально назначенный общедоступный IP - адрес.

Имеющие право клиенты

Распределение нагрузки является эффективным только на удаленных сеансах, инициируемых с этими клиентами:

- Cisco VPN Client (выпуск 3.0 или позже)
- Аппаратный клиент Cisco VPN 3002 (выпуск 3.5 или позже)
- CiscoASA 5505 при действии как Клиент Easy VPN

Все другие клиенты, включая прямые соединения локальных сетей, могут соединиться с устройством безопасности, на котором включено распределение нагрузки, но они не могут участвовать в распределении нагрузки.

Используемые компоненты

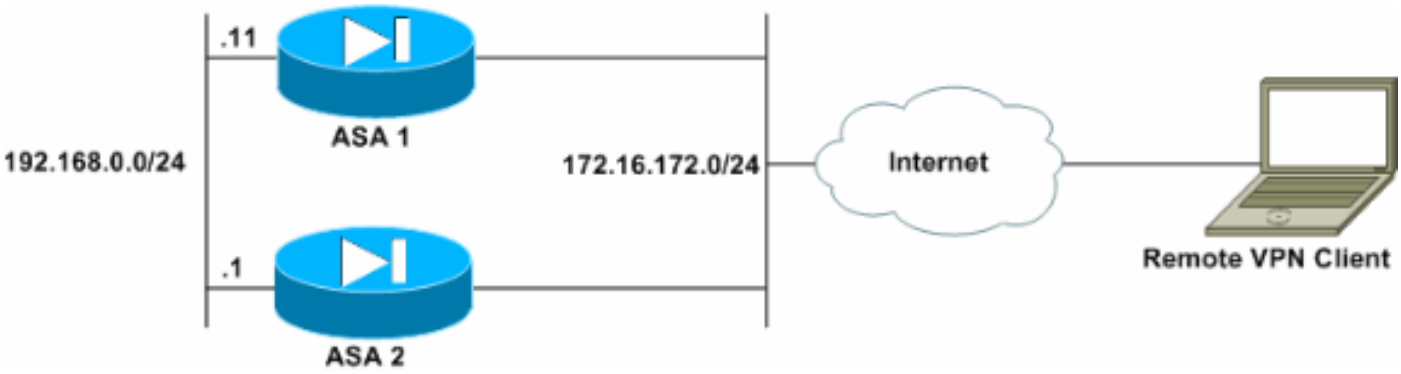
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версии ПО Cisco VPN Client 4.6 и позже
- Выпуски ПО Cisco ASA 7.0.1 и позже**Примечание:** Расширяет поддержку распределения нагрузки ASA 5510 и моделям ASA позже, чем 5520, которые имеют Безопасность Плюс лицензия с 8.0 (2) версия.

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.

Схема сети

В настоящем документе используется следующая схема сети:



Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Ограничения

- IP-адрес виртуального кластера сети VPN, порт протокола датаграмм пользователя

(UDP) и общий секретный ключ должны совпадать на всех устройствах, входящих в состав виртуального кластера.
- Все устройства в виртуальном кластере должны быть на тех же внутренних и внешних IP-подсетях.

!--- конфигурацию

Назначение IP-адресов

Гарантируйте, что IP-адреса настроены на внутренних и внешних интерфейсах, и вы в состоянии добраться до Интернета от вашего ASA.

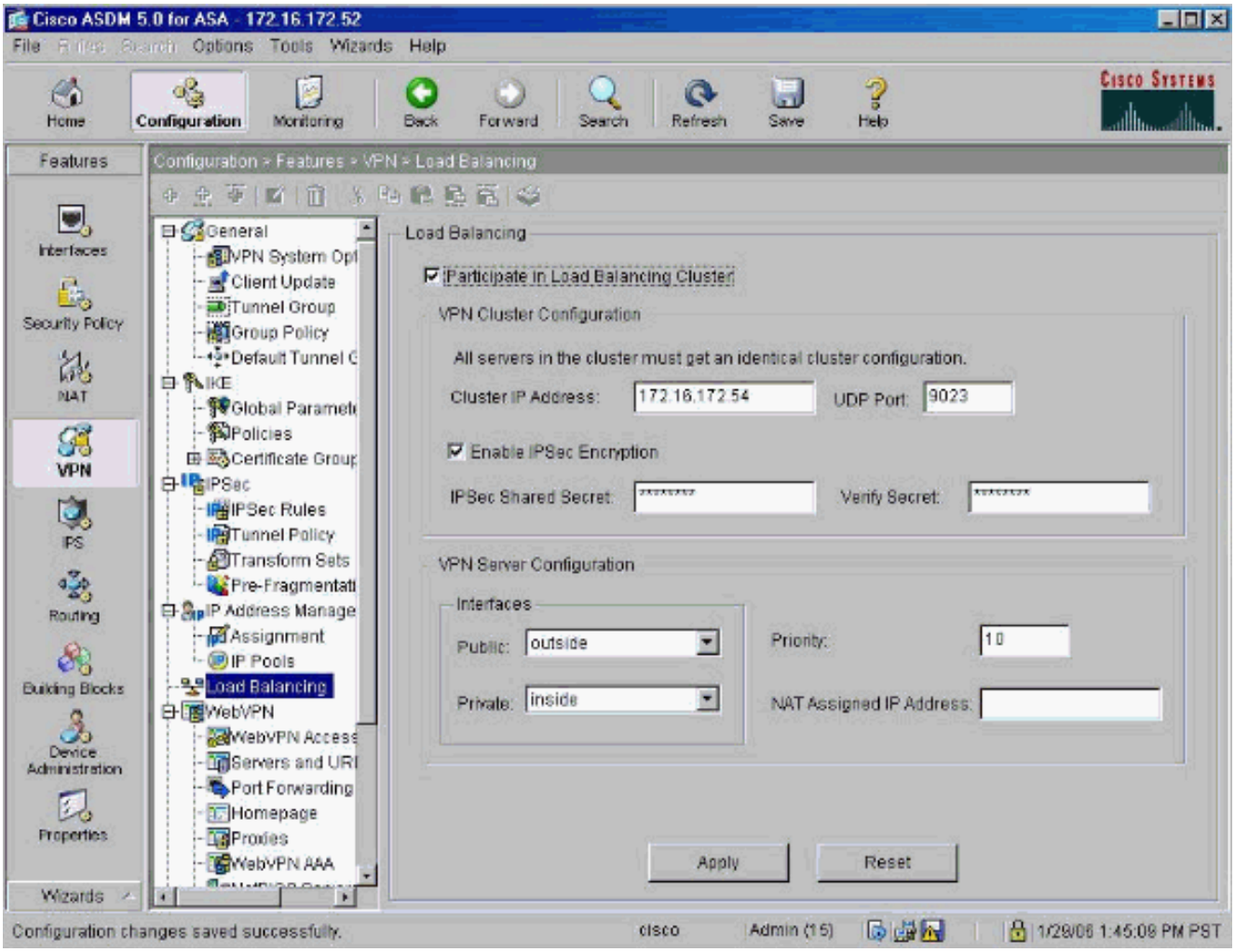
Примечание: Гарантируйте, что ISAKMP включен на обоих внутренние и внешние интерфейсы. Выберите **Configuration> Features> VPN> IKE> Global Parameters** для проверки этого.

Конфигурация кластера

Эта процедура показывает, как использовать Cisco Adaptive Security Device Manager (ASDM) для настройки распределения нагрузки.

Примечание: Многие параметры в данном примере имеют значения по умолчанию.

1. Выберите **Configuration> Features> VPN> Load Balancing**, и проверка **Участвует в Распределении нагрузки Кластера** для включения распределения нагрузки VPN.



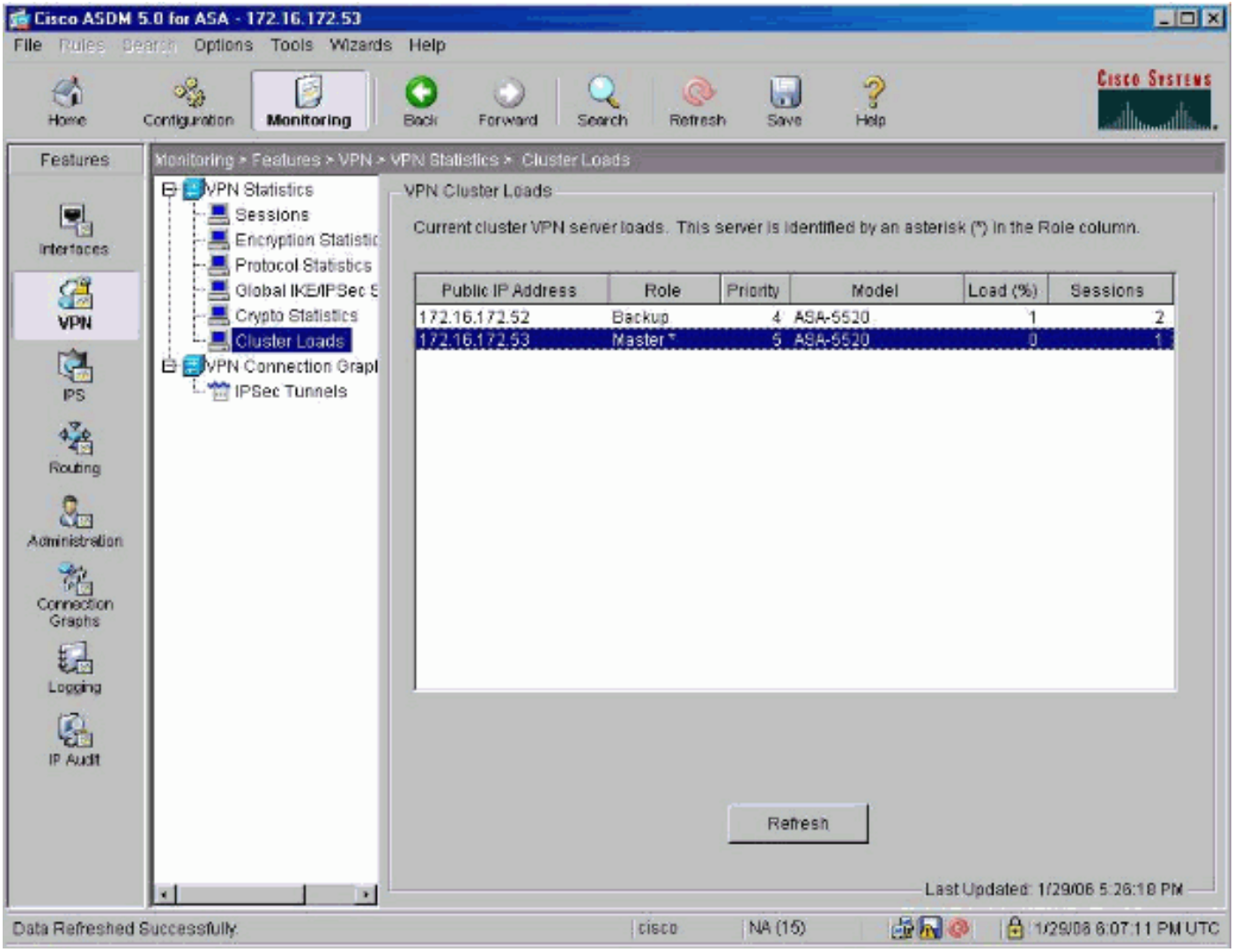
2. Выполните эти шаги для настройки параметров для всех ASA, участвующих в кластере в Групповом блоке Конфигурации кластера VPN:Введите IP-адрес кластера в Кластерном текстовом поле IP-адреса.Нажмите **Enable IPSec Encryption**.Введите ключ шифрования в текстовом поле Общего секрета IPsec и введите его снова в Сверять Секретном текстовом поле.
3. Настройте опции в коробке Группы конфигурации Сервера VPN:Выберите интерфейс, который принимает входящие VPN-подключения в Общем списке.Выберите интерфейс, который является частным интерфейсом в Частном списке.*(Необязательно)* Изменяют приоритет, который ASA имеет в кластере в Приоритетном текстовом поле.Введите IP-адрес для Назначенного IP - адреса Технологии NAT, если это устройство находится позади межсетевого экрана, который использует NAT.
4. Повторите шаги во все участвующие ASA в группе.

Пример в этом разделе использует эти команды CLI для настройки распределения нагрузки:

```
VPN-ASA2(config)#vpn load-balancing VPN-ASA2(config-load-balancing)#priority 10 VPN-ASA2(config-load-balancing)#cluster key cisco123 VPN-ASA2(config-load-balancing)#cluster ip address 172.16.172.54 VPN-ASA2(config-load-balancing)#cluster encryption VPN-ASA2(config-load-balancing)#participate
```

Мониторинг

Выберите **Monitoring> Features> VPN> VPN Statistics> Cluster Loads** для мониторинга функции распределения нагрузки на ASA.



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **покажите, что распределение нагрузки vpn** — Проверяет функцию распределения нагрузки VPN.`Status: enabled`
`Role: Backup`
`Failover: n/a`
`Encryption: enabled`
`Cluster IP: 172.16.172.54`
`Peers: 1`

```
Public IP Role Pri Model Load (%) Sessions
-----------------------------------------------------------
* 172.16.172.53 Backup 5 ASA-5520 0 1
172.16.172.52 Master 4 ASA-5520 n/a n/a
```

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **vpnlb 250 отладки** — Используемый для устранения проблем функции распределения нагрузки VPN.VPN-ASA2#

```
VPN-ASA2# 5718045: Created peer[172.16.172.54]
5718012: Sent HELLO request to [172.16.172.54]
5718016: Received HELLO response from [172.16.172.54]
7718046: Create group policy [vpnlb-grp-pol]
7718049: Created secure tunnel to peer[192.168.0.11]
5718073: Becoming slave of Load Balancing in context 0.
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718035: Received TOPOLOGY indicator from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
```

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация