Пример конфигурации управление пропускной способностью концентратора VPN 3000

Содержание

Введение

Этот документ описывает обязательные действия, используемые для настройки Характеристики управления пропускной способностью на Cisco VPN 3000 Concentrator для:

- От узла к узлу (LAN-LAN) VPN-туннели
- Туннели VPN для удаленного доступа

Примечание: Перед настройкой удаленного доступа или туннелей VPN типа «узел-узел» необходимо сначала настроить политику полосы пропускания по умолчанию по VPN 3000 Concentrator.

Существует два элемента Управления пропускной способностью:

- **Применение политик пропускной способности** — Ограничивает максимальное значение туннельного трафика. Концентратор VPN передает трафик, который он получает ниже этой скорости и отбрасывает трафик, который превышает эту скорость.
- **Резервирование полосы пропускания** — Откладывает скорость минимальной пропускной способности для туннельного трафика. Управление пропускной способностью позволяет вам выделять пропускную способность группам и пользователям справедливо. Это препятствует тому, чтобы определенные группы или пользователи использовали большинство пропускной способности.

Управление пропускной способностью применяется только к туннельному трафику (Протокол туннелирования уровня 2 [L2TP], Протокол туннелирования "Точка-точка" [PPTP],

IPSec) и обычно применено к открытому интерфейсу.

Характеристика управления пропускной способностью предоставляет административные преимущества для удаленного доступа и сквозных VPN-соединение соединений. Туннели VPN для удаленного доступа используют Применение политик Пропускной способности так, чтобы пользователи широкополосной связи не использовали всю пропускную способность. С другой стороны администратор может настроить Резервирование полосы пропускания для туннелей от узла к узлу для гарантии минимальной ширины полосы пропускания каждому удаленному узлу.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

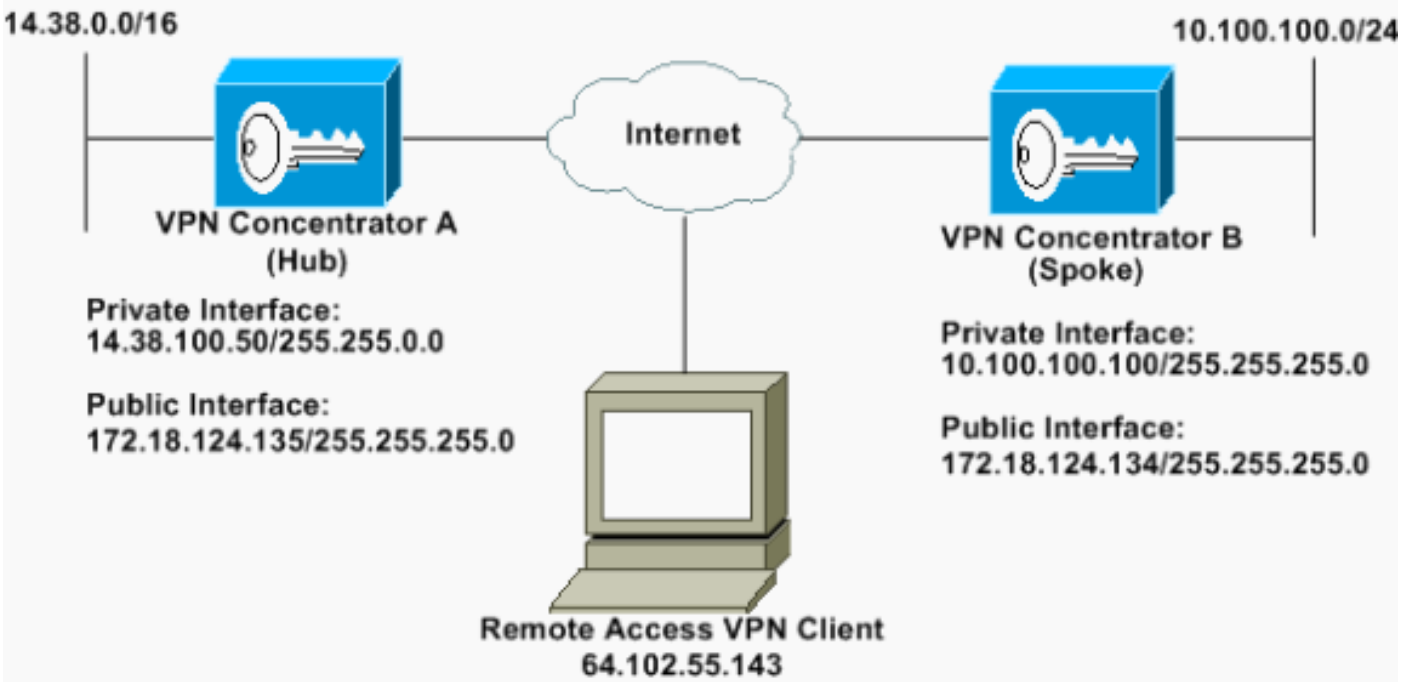
- Cisco VPN 3000 Concentrator с Выпусками ПО 4.1.x и позже

Примечание: Характеристика управления пропускной способностью была представлена в выпуске 3.6.

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:



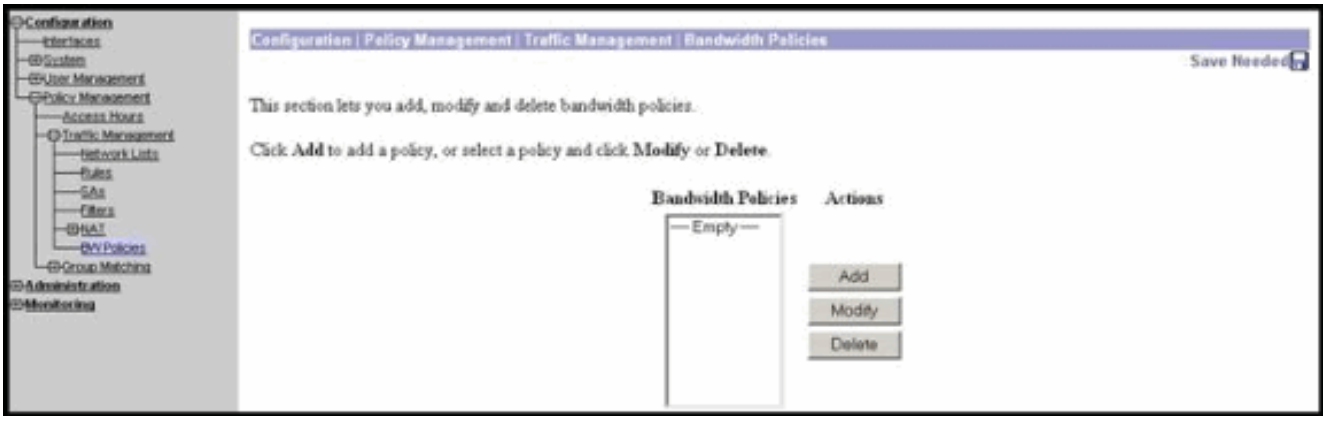
Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

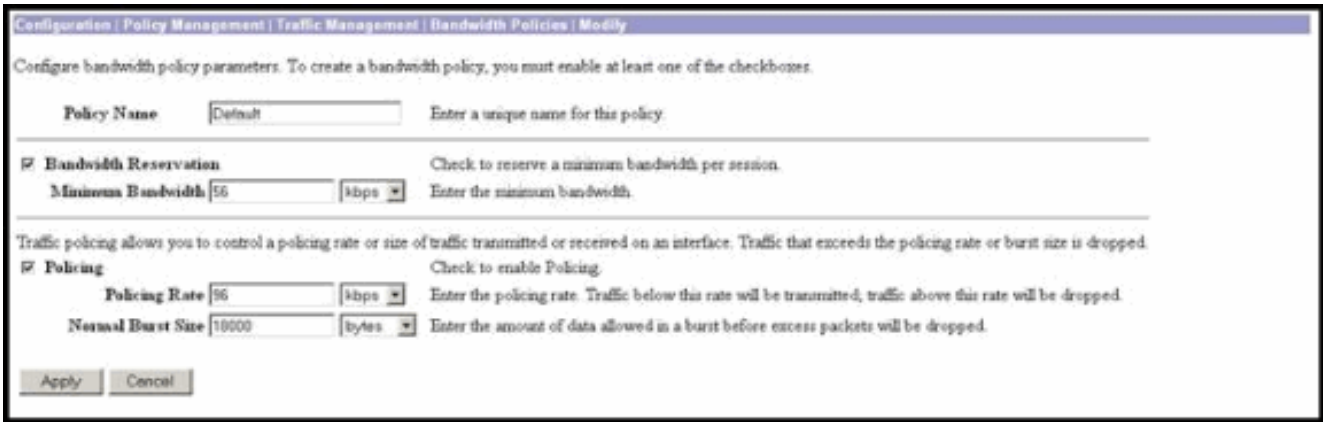
Настройте политику полосы пропускания по умолчанию по VPN 3000 Concentrator

Прежде чем можно будет настроить Управление пропускной способностью на туннелях между локальными сетями (LAN-to-LAN) или на туннелях удаленного доступа, необходимо включить Управление пропускной способностью на открытом интерфейсе. В этом примере конфигурации настроена политика полосы пропускания по умолчанию. Эта политика по умолчанию применена к пользователям/туннелям, которым не применились к политике Управления пропускной способностью группа, которой они принадлежат в Концентраторе VPN.

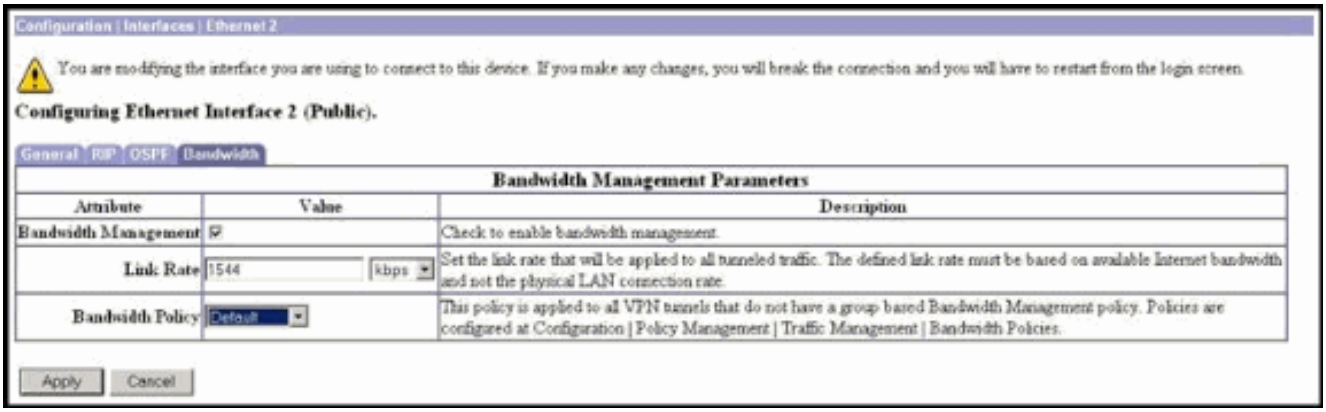
1. Для настройки политики выберите **Configuration> Policy Management> Traffic Management> Bandwidth Policies** и **нажмите Add**.



После того, как вы нажмите Add, окно Modify отображено.



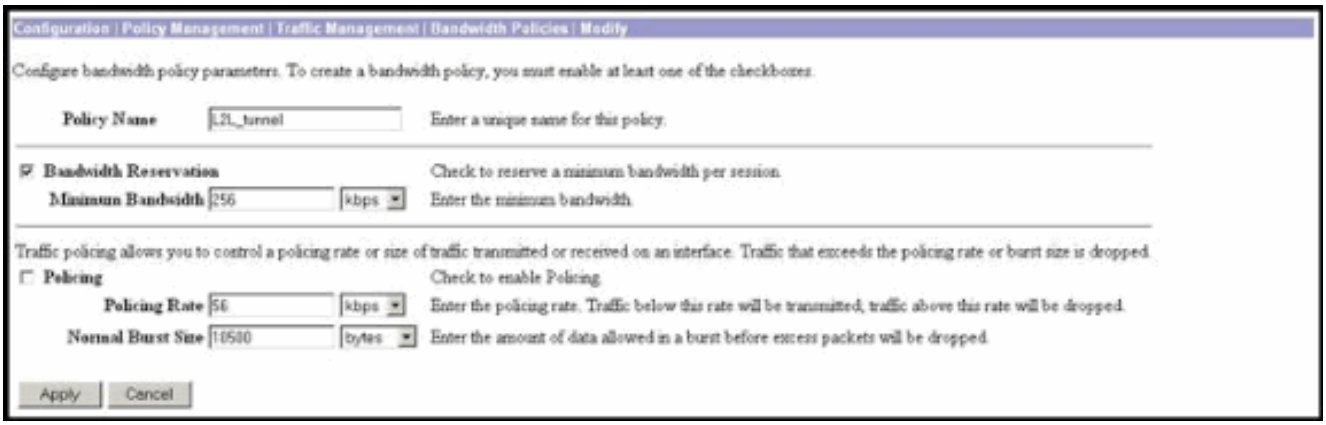
2. Установите эти параметры в окне Modify.**Название политики** — Вводит имя уникальной политики, которое может помочь вам помнить политику. Максимальная длина составляет 32 символа. В данном примере название 'По умолчанию' настроено как Название Политики.**Резервирование полосы пропускания** — Проверка флажок **Bandwidth Reservation** для резервирования минимальной ширины полосы пропускания для каждого сеанса. В данном примере 56 кбит/с пропускной способности зарезервированы для всех пользователей VPN, которые не подпадают под группу, которой настроили Управление пропускной способностью.**Применение политик** — Проверка флажок **Policing**, чтобы позволить определить политику. Введите значение для Ограничения скорости и выберите единицу измерения. Концентратор VPN передает трафик, который перемещается ниже ограничения скорости и отбрасывает весь трафик, который перемещается выше ограничения скорости. 96 кбит/с настроены для Применения политик Пропускной способности. Обычный размер пакета является суммой мгновенного пакета, который Концентратор VPN может передать в любое заданное время. Для установки размера пакета используйте эту формулу:`(Policing Rate/8) * 1.5`С этой формулой Пиковая скорость составляет 18000 байтов.
3. **Щелкните "Применить".**
4. Выберите **Configuration> Interfaces> Public Interface** и щелкните по вкладке Bandwidth для применения политики полосы пропускания по умолчанию к интерфейсу.
5. Включите опцию **Bandwidth Management**.
6. Задайте скорость соединения.Скорость соединения является скоростью сетевого подключения через Интернет. В данном примере используется соединение T1 с Интернетом. Следовательно, 1544 кбит/с скорость настраиваемого соединения.
7. Выберите политику от выпадающего списка Политиков пропускной способности.Политика по умолчанию настроена ранее для этого интерфейса. Политика, которую вы применяете здесь, является политикой полосы пропускания по умолчанию для всех пользователей на этом интерфейсе. Эта политика применена к пользователям, которым не применились к политике Управления пропускной способностью их
группа.



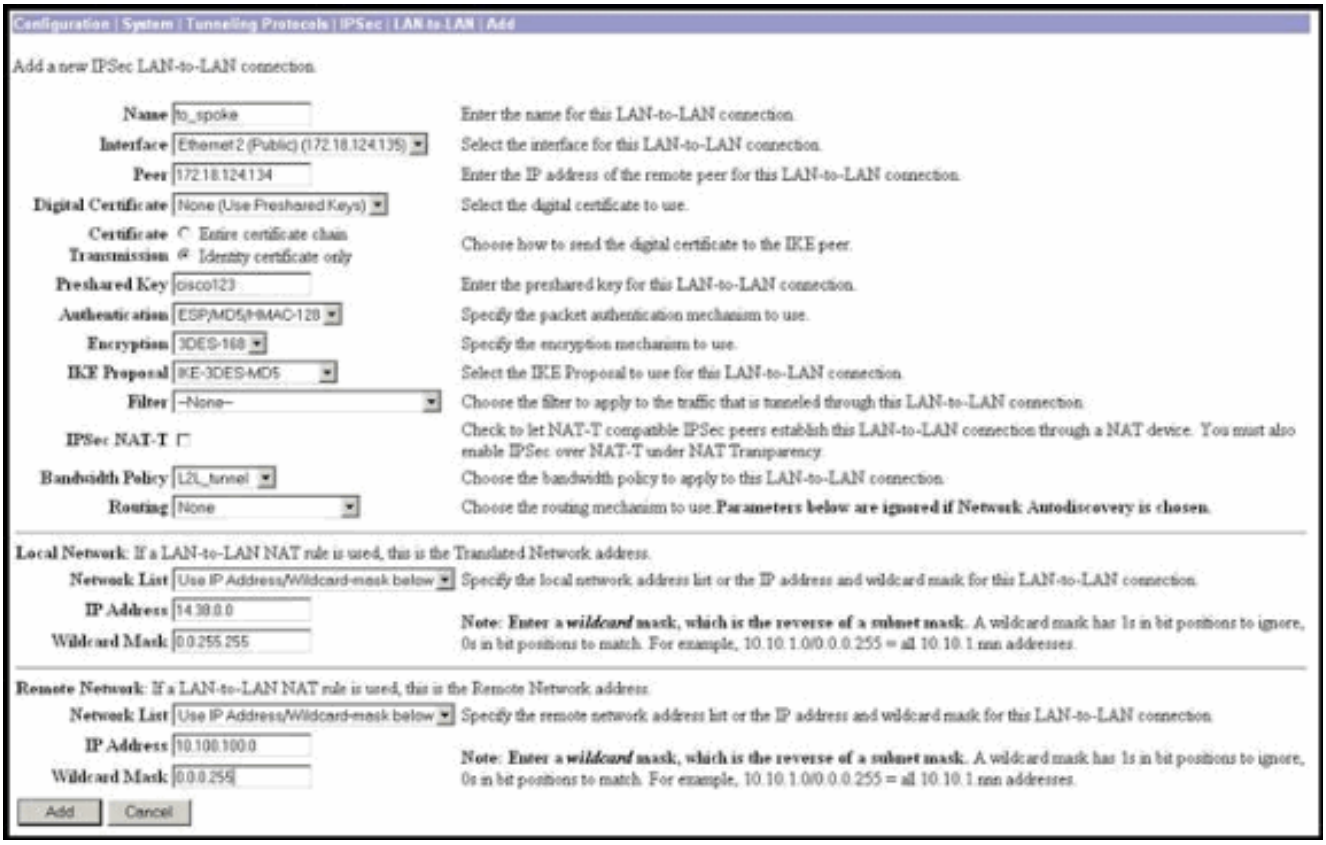
Настройте управление пропускной способностью для туннелей от узла к узлу

Выполните эти шаги для настройки Управления пропускной способностью для туннелей от узла к узлу.

1. Выберите **Configuration> Policy Management> Traffic Management> Bandwidth Policies** и **нажмите Add** для определения новых политиков пропускной способности LAN-LAN.В данном примере политика по имени 'L2L_tunnel' была настроена с резервированием полосы пропускания 256
кбит/с.



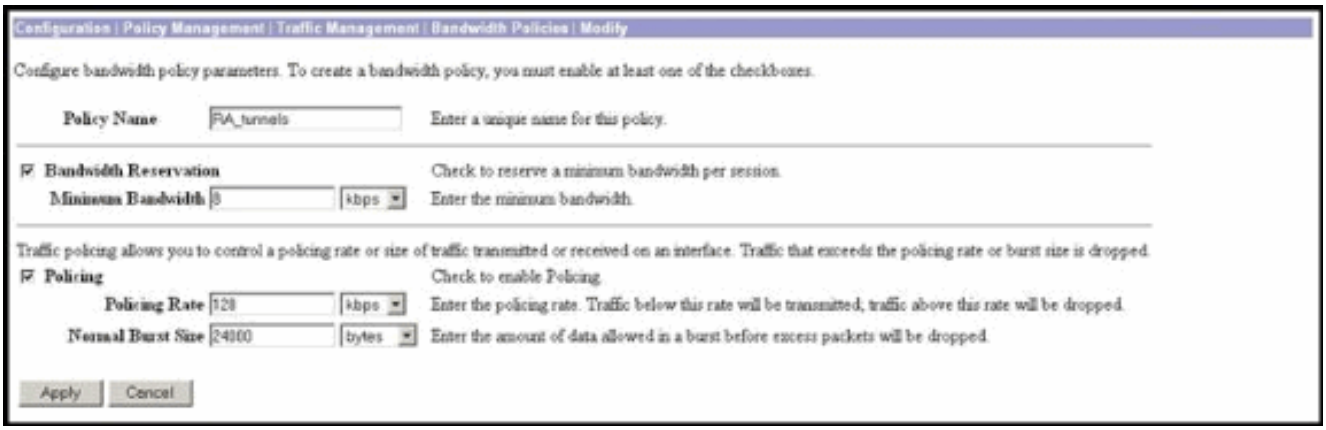
2. Примените политиков пропускной способности к существующему туннелю между локальными сетями (LAN-to-LAN) под раскрывающимся меню Политиков пропускной способности.



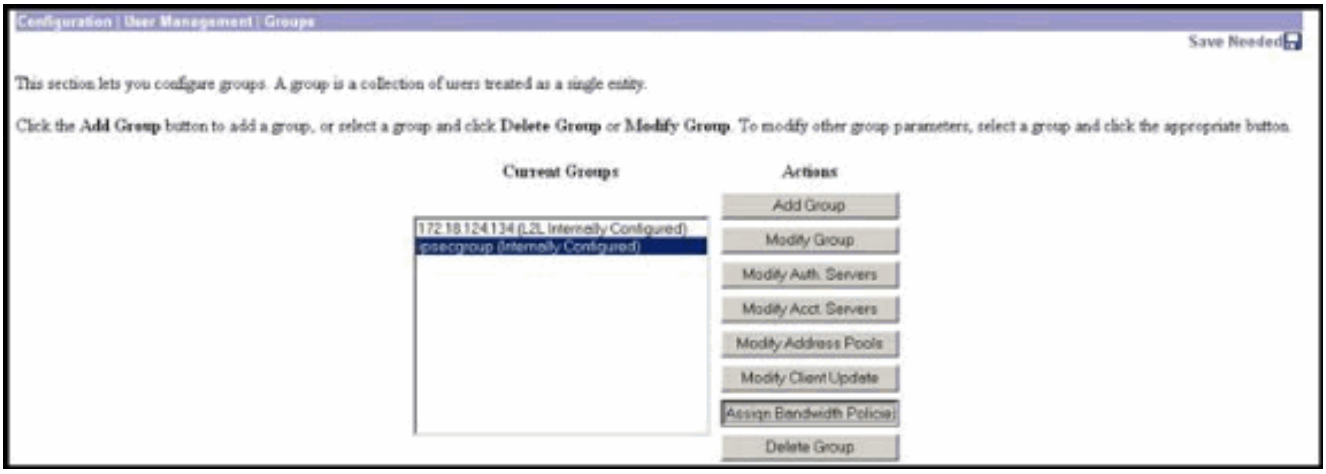
Настройте управление пропускной способностью для удаленных VPN-туннелей

Выполните эти шаги для настройки Управления пропускной способностью для удаленных VPN-туннелей.

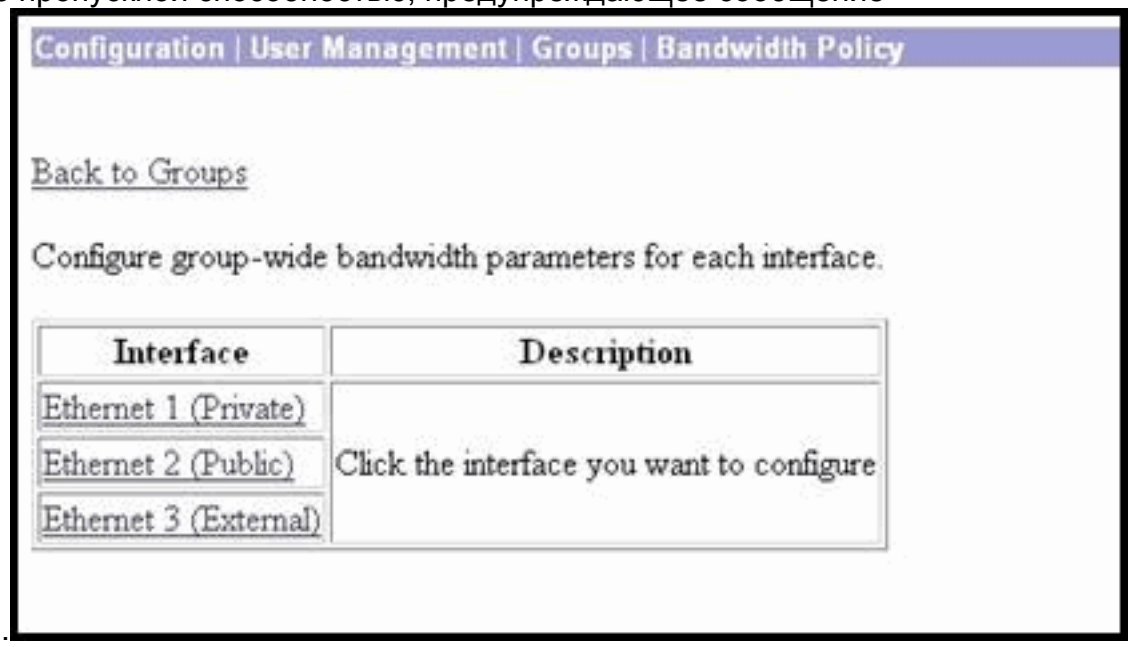
1. Выберите **Configuration> Policy Management> Traffic Management> Bandwidth Policies** и **нажмите Add** для создания новых политиков пропускной способности.В данном примере политика под названием 'RA_tunnels' настроена с резервированием полосы пропускания 8 кбит/с. Мониторинг трафика настроен с ограничением скорости 128 кбит/с и размером пакета 24000
байтов.



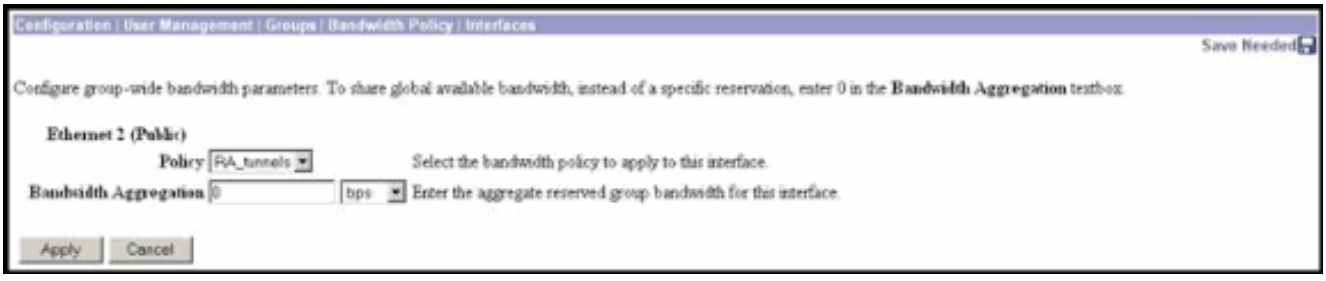
2. Для применения политиков пропускной способности к группе VPN для удаленного доступа выберите **Configuration> User Management> Groups**, выберите группу и нажмите **Assign Bandwidth
Policies**.



3. Нажмите интерфейс, на котором вы хотите настроить Управление пропускной способностью для этой группы.В данном примере, 'Ethernet2 (Общественность)' является выбранным интерфейсом для группы. Для применения политиков пропускной способности к группе на интерфейсе Управлению пропускной способностью нужно включить на том интерфейсе. Если вы выбираете интерфейс, на котором отключено Управление пропускной способностью, предупреждающее сообщение появляется.

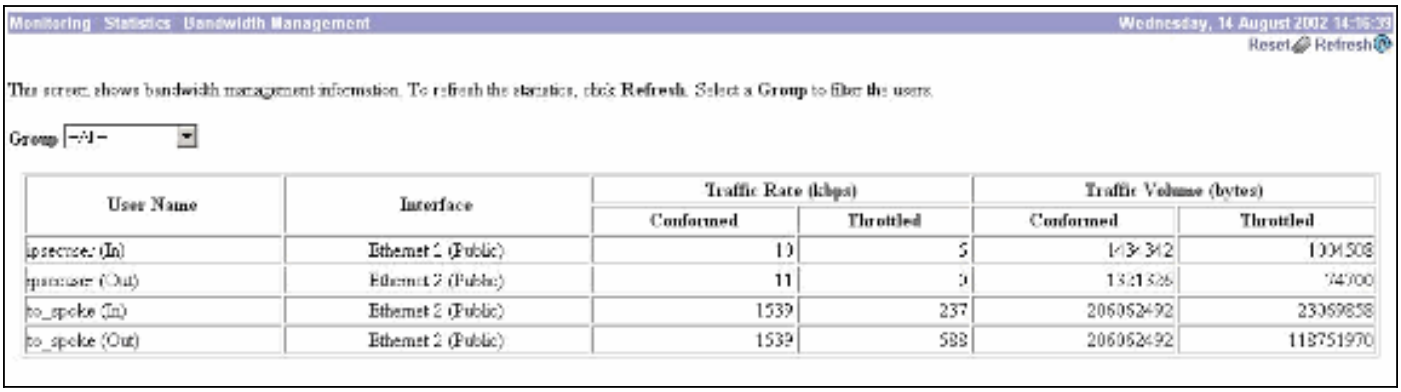


4. Выберите политиков пропускной способности для группы VPN для этого интерфейса.Политика RA_tunnels, которая была ранее определена, выбрана для этой группы. Введите значение для минимальной пропускной способности для резервирования для этой группы. Значение по умолчанию Агрегирования полос пропускания 0. Единица измерения по умолчанию является битом в секунду. Если вы хотите, чтобы группа совместно использовала в доступной пропускной способности на интерфейсе, войдите
0.



Проверка

Выберите **Monitoring> Statistics> Bandwidth Management** на VPN 3000 Concentrator для мониторинга Управления пропускной способностью.



Устранение неполадок

Для устренения любых проблем, в то время как Управление пропускной способностью внедрено на VPN 3000 Concentrator включите эти два Класса события под **Configuration> System> Events> Classes**:

- **BMGT** (со степенями серьезности ошибки для Регистрации: 1-9)
- **BMGTDBG** (со степенями серьезности ошибки для Регистрации: 1-9)

Это некоторые наиболее распространенные сообщения журнала регистрации событий:

- Когда Политики пропускной способности модифицируются, сообщение об ошибках `Exceeds the Aggregate Reservation` замечено на журналах.
  ```
  1 08/14/2002 10:03:10.840 SEV=4 BMGT/47 RPT=2
  The Policy [ RA_tunnels ] with Reservation [ 8000 bps ] being
  applied to Group [ipsecgroup ] on Interrface [ 2 ] exceeds
  the Aggregate Reservation [ 0 bps ] configured for that group.
  ```
  Если это сообщение об ошибках отображено, возвратитесь к параметрам группы и не примените политику 'RA_tunnel' от группы. Отредактируйте 'RA_tunnel' с правильными значениями и затем повторно примените политику назад определенной группе.
- Неспособный найти полосу пропускания интерфейса.
  ```
  11 08/14/2002 13:03:58.040 SEV=4 BMGTDBG/56 RPT=1
  Could not find interface bandwidth policy 0 for group 1 interface 2.
  ```
  Можно получить эту ошибку, если политики пропускной способности не включены на интерфейсе, и вы пытаетесь применить его на туннель между локальными сетями (LAN-to-LAN). Если это верно, примените политику к открытому интерфейсу, как объяснено в Настраивании Политики Полосы пропускания по умолчанию по разделу VPN 3000 Concentrator.

Дополнительные сведения

- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Series Client
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems