7PIX/ASA: Пример конфигурации прозрачного межсетевого экрана

Содержание

Введение

Традиционно межсетевой экран представляет собой маршрутизируемый переход и по умолчанию функционирует как шлюз для узлов, подключенных к одной из защищенных им подсетей. Прозрачный межсетевой экран, с другой стороны, представляет собой межсетевой экран уровня 2, который работает как **устройство с аппаратной реализацией безопасности (BITW, bump in the wire)** или "**невидимый межсетевой экран**", поскольку не воспринимается подключенными устройствами как маршрутизируемый переход. Устройство защиты подключается к одной и той же сети на своих внутренних и внешних портах. Так как межсетевой экран не является маршрутизируемым переходом, можно с легкостью встроить прозрачный межсетевой экран в сеть, не прибегая к изменению IP-адресации.

Его поддержка значительно облегчается, так как не требуется устранять проблемы, связанные со сложными шаблонами маршрутизации или настройкой NAT.

Несмотря на то, что функционирование в режиме прозрачности напоминает работу моста, трафик уровня 3, например, IP-трафик, не может проникнуть сквозь устройство защиты, если не было явно заданного разрешения на выполнение этого действия, сопровожденного расширенным списком доступа. Единственный трафик, для которого возможно прохождение через прозрачный межсетевой экран без списка доступа — это трафик ARP. Проверка ARP-трафика осуществляется с помощью функции инспектирования ARP.

В маршрутизируемом режиме некоторые виды трафика не могут быть пропущены устройством защиты, даже если они разрешены списком доступа. Кроме того, прозрачный межсетевой экран пропускает любой трафик из расширенного списка доступа (IP-трафик) или списка доступа EtherType (трафик, отличный от IP-трафика).

Например, с помощью прозрачного межсетевого экрана можно установить смежности протокола маршрутизации; также можно разрешить прохождение трафика VPN (IPSec), OSPF, RIP, EIGRP или BGP на основании расширенного списка доступа. Точно так же

протоколы, например, HSRP или VRRP, могут быть пропущены через устройство защиты.

Для трафика, отличного от IP трафика (например, AppleTalk, IPX, BPDU и MPLS), можно задать конфигурацию для прохождения на основании списка доступа EtherType.

Если какие-либо функции не поддерживаются прозрачным межсетевым экраном, можно разрешить прохождение трафика через него, чтобы восходящие или нисходящие маршрутизаторы смогли обеспечить необходимую функциональность. Например, можно разрешить прохождение DHCP-трафика в расширенном списке доступа (вместо неподдерживаемой функции переключения DHCP) или многоадресный трафик, который создается IP/TV.

Если устройство защиты работает в прозрачном режиме, исходящий интерфейс пакета определяется с помощью поиска MAC-адреса, а не с помощью поиска маршрута. Инструкции маршрута можно настроить, однако они применимы только для трафика, созданного устройством защиты. Например, если сервер системного журнала расположен в удаленной сети, необходимо использовать статический маршрут, чтобы устройство защиты могло достичь данной подсети.

Устройство адаптивной защиты может быть настроено для работы в режиме маршрутизируемого межсетевого экрана по умолчанию или в режиме прозрачного межсетевого экрана. При смене режимов устройство адаптивной защиты очищает конфигурацию, так как многие команды поддерживаются только в одном из режимов. Если заполненная конфигурация уже имеется, сохраните ее перед тем, как изменить режим; сохраненную конфигурацию можно использовать для справки при создании новой конфигурации.

В многоконтекстном режиме возможно использование только одного межсетевого экрана для всех контекстов. Режим необходимо указать в системном поле выполнения. В многоконтекстном режиме конфигурация системы стирается, при этом все контексты удаляются. При добавлении контекста с уже существующей конфигурацией, заданной для другого режима, конфигурация контекста не будет работать корректно.

Примечание. Убедитесь, что конфигурации контекстов созданы для соответствующего режима до того, как они будут добавлены, или добавляйте новые контексты с новыми путями для новых конфигураций.

Примечание. Если для устройства защиты была загружена текстовая конфигурация, которая изменила режим с помощью команды **firewall transparent**, убедитесь, что она находится в верхней части текста конфигурации. Устройство адаптивной защиты изменяет режим сразу после исполнения команды, а затем продолжает чтение загруженной конфигурации. Если команда расположена ниже части текста конфигурации, устройство адаптивной защиты удалит все предыдущие строки конфигурации.

Дополнительные сведения о настройке многоконтекстного режима прозрачного межсетевого экрана, см. в разделе Многоконтекстный режим, прозрачный межсетевой экран с внешним доступом

Предварительные условия

Требования

Настоящий документ не предъявляет каких-либо специфических требований.

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к следующим версиям программного и аппаратного обеспечения:

- Адаптивная система безопасности (ASA) версии 7.x и более поздняя

Данные для документа были получены в специально созданных лабораторных условиях. Все упоминаемые устройства первоначально работали в конфигурации по умолчанию. Если сеть работает в реальных условиях, следует адекватно оценивать возможные последствия использования каждой команды.

Соответствующие продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения.

- Устройство защиты PIX Security Appliance версии 7.x и выше

Условные обозначения

Подробные сведения о применяемых в документе обозначениях см. в статье Условные обозначения, используемые в технической документации Cisco.

Прозрачный межсетевой экран

Рекомендации

Следуйте данным рекомендациям при планировании сети с прозрачным межсетевым экраном:

- Необходимо наличие управляющего IP-адреса; для многоконтекстного режима IP-адрес обязателен для каждого контекста.

  В отличие от маршрутизируемого режима, в котором требуется IP-адрес для каждого интерфейса, в прозрачном межсетевом экране имеется IP-адрес, назначенный для всего устройства. Устройство защиты использует этот IP-адрес в качестве исходного адреса для пакетов, созданных устройством защиты, таких как системные сообщения или сообщения авторизации, аутентификации и учета (AAA).

  Управляющий IP-адрес должен принадлежать той же подсети, что подключенная сеть. Не допускается устанавливать подсеть равной подсети хоста (255.255.255.255).

- Прозрачное устройство защиты использует только внутренний и внешний интерфейс. Если у платформы имеется выделенный интерфейс управления, можно выполнить настройку интерфейса управления или подчиненного интерфейса только для пропускания трафика управления.

  В одиночном режиме можно использовать два интерфейса данных (а также выделенный интерфейс управления, если он доступен) даже в том случае, если устройство защиты включает в себя более двух интерфейсов.

- Каждая напрямую подключенная сеть должна быть расположена в той же подсети.

- Не допускается указывать управляющий IP-адрес устройства защиты в качестве шлюза по умолчанию для подключенных устройств. В качестве шлюза по умолчанию для устройств должен быть определен маршрутизатор на другой стороне устройства защиты.

- В многоконтекстном режиме каждый контекст должен использовать различные интерфейсы, несколько контекстов не могут использовать один интерфейс.

- В многоконтекстном режиме для каждого контекста обычно используются разные подсети. Можно использовать перекрывающиеся подсети, однако для сетевой топологии обязательно наличие маршрутизатора и конфигурации NAT, чтобы это было осуществимо с точки зрения маршрутизации.

- Необходимо использовать расширенный список доступа для разрешения прохождения через устройство защиты трафика уровня 3, например, IP-трафика.

  Также можно использовать список доступа EtherType для разрешения пропуска трафика, отличного от IP.

Разрешенные MAC-адреса

Эти MAC-адреса назначения разрешены для прохождения трафика через прозрачный межсетевой экран. Любые MAC-адреса, не указанные в данном списке, отбрасываются.

- Широковещательные MAC-адреса назначения TRUE равны FFFF.FFFF.FFFF

- MAC-адреса многоадресной рассылки IPv4 с 0100.5E00.0000 по 0100.5EFE.FFFF

- MAC-адреса многоадресной рассылки IPv6 с 3333.0000.0000 по 3333.FFFF.FFFF
- Адрес многоадресной рассылки BPDU, равный 0100.0CCC.CCCD
- Многоадресные MAC-адреса AppleTalk с 0900.0700.0000 до 0900.07FF.FFFF

Не поддерживаемые функции

Следующие функции не поддерживаются в прозрачном режиме:

- NAT/PAT

  NAT выполняется в маршрутизаторе восходящего потока.

- Протоколы динамической маршрутизации (RIP, EIGRP, OSPF)

  Допускается добавление статических маршрутов для трафика, созданного устройством защиты. Также можно разрешить прохождение трафика протоколов динамической маршрутизации через устройство защиты, с помощью расширенных списков доступа.

- IPv6
- Ретрансляция DHCP

  Прозрачный межсетевой экран может выступать в качестве DHCP-сервера, но при этом он не поддерживает выполнение команд ретрансляции DHCP. Ретрансляция DHCP не требуется, поскольку для пропуска DHCP-трафика можно использовать расширенный список доступа.

- Качество обслуживания (QOS)
- Многоадресная рассылка

  Многоадресный трафик может быть разрешен для прохождения через устройство защиты с помощью расширенного списка доступа.

- Прерывание проходящего трафика в VPN

  Прозрачный межсетевой экран поддерживает VPN-туннели типа "узел-узел" только для соединений управления. Он не выполняет прерывание соединений VPN для трафика, проходящего через устройство защиты. Можно разрешить прохождение трафика VPN через устройство защиты с помощью расширенного списка доступа, однако прерывания соединений, не относящихся к управлению, выполняться не будет.

Примечание. В прозрачном режиме устройство защиты не пропускает CDP-пакеты или любые другие пакеты, не имеющие допустимого значения EtherType, большего или равного 0x600. Например, невозможно прохождение пакетов IS-IS. Исключение составляют поддерживаемые блоки данных протокола моста (BPDUs), которые поддерживаются.

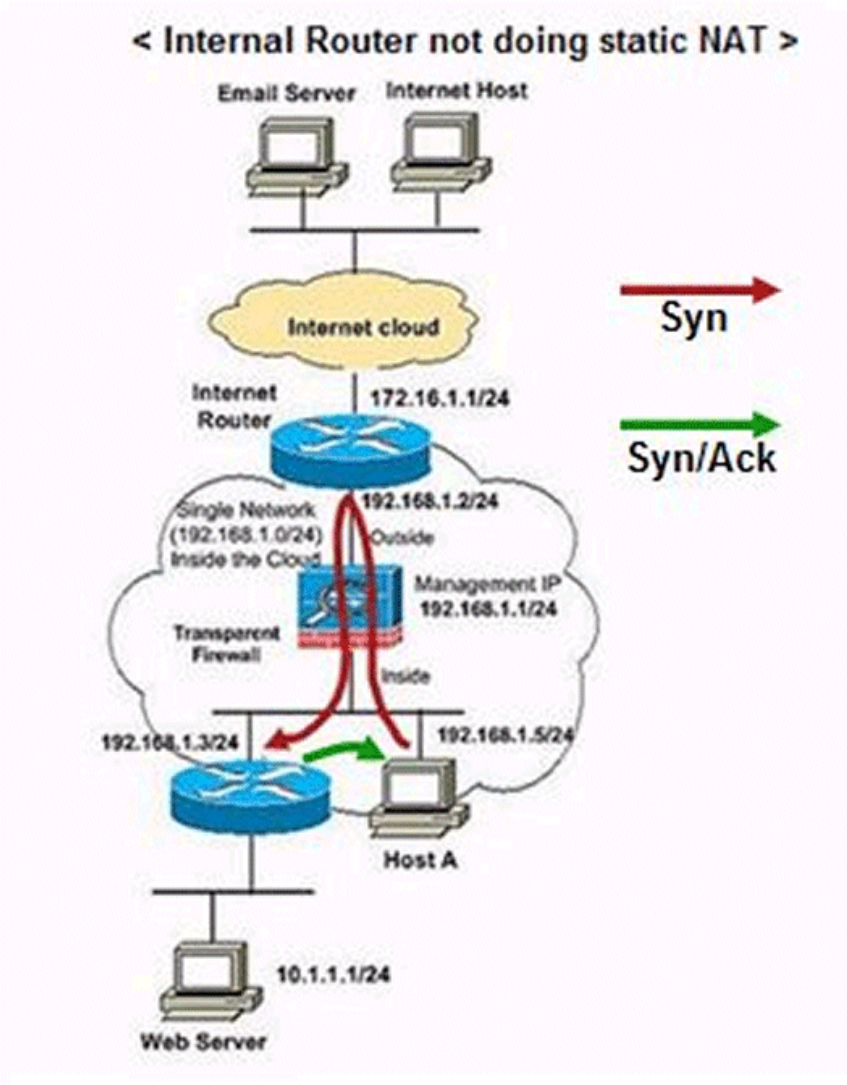
Настройка

В этом разделе приводится информация по настройке функций, описанных в данном документе.

Примечание. Воспользуйтесь Средством поиска команд (только для зарегистрированных клиентов) для получения дополнительных сведений о командах, упомянутых в этом разделе.

Схема сети

На схеме сети представлена типичная сеть с прозрачным межсетевым экраном, в которой внешние устройства расположены в той же подсети, что и внутренние. Внутренний маршрутизатор и узлы подключены напрямую к внешнему маршрутизатору.



Конфигурации

ASA 8.x

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
!--- Чтобы настроить межсетевой экран на прозрачный режим

firewall transparent
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
!
interface Ethernet0/1
nameif inside
security-level 100
!
interface Ethernet0/2
shutdown
no nameif
no security-level
!
interface Ethernet0/3
shutdown
no nameif
no security-level
!
```

```
interface Management0/0
shutdown
no nameif
no security-level
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500

!--- IP-адрес для управления.
!--- Не используйте этот IP-адрес в качестве шлюза по умолчанию.
!--- Устройство защиты использует этот IP-адрес в качестве исходного адреса
!--- для трафика, созданного самим устройством, например для системных
!--- сообщений или обмена данными с AAA-серверами. Можно также использовать этот
!--- адрес для удаленного управления.


ip address 192.168.1.1 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1


!--- Выходные данные команды опущены.



service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ciscoasa(config)#
```

Различные сценарии перемещения данных в прозрачном межсетевом экране

Получение доступа к внешнему серверу электронной почты внутренним пользователем

Пользователь внутренней сети получает доступ к серверу электронной почты в Интернете (внешнему). Устройство защиты получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, система проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание. В многоконтекстном режиме устройство защиты вначале определяет пакет в соответствии с уникальным интерфейсом.

Устройство защиты заносит в журнал запись о созданном сеансе. Если MAC-адрес назначения присутствует в таблице, устройство защиты передает пакет наружу, через один из внешних интерфейсов. В качестве MAC-адрес назначения используется адрес маршрутизатора восходящего потока, 192.168.1.2. Если MAC-адрес назначения отсутствует в таблице устройства защиты, то устройство пытается его обнаружить при отправке запроса ARP и эхо-запроса. Первый пакет отбрасывается.

Сервер электронной почты отвечает на запрос; поскольку сеанс уже выполняется, пакет обходит множество операций поиска, связанных с новым соединением. Устройство защиты отправляет пакет внутреннему пользователю.

Посещение внутренним пользователем веб-сервера с NAT

При включении NAT на маршрутизаторе, подключенном к Интернету, поток направляемых через него пакетов незначительно изменяется.

Пользователь внутренней сети получает доступ к серверу электронной почты в Интернете (снаружи сети). Устройство защиты получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, система проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание. В многоконтекстном режиме устройство защиты сначала идентифицирует пакет, в соответствии с уникальным интерфейсом.

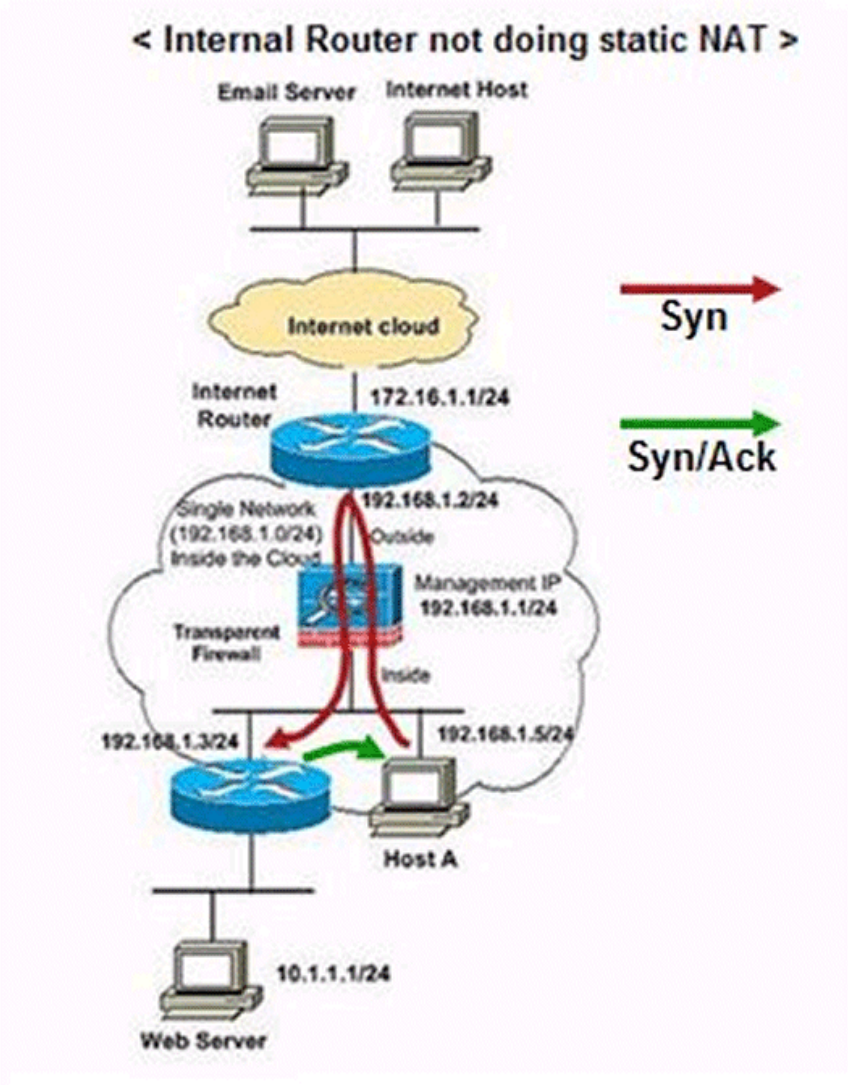
Маршрутизатор Интернета преобразует фактический адрес узла A (192.168.1.5) в сопоставленный адрес маршрутизатора Интернета (172.16.1.1). Поскольку сопоставленный адрес не принадлежит к той же сети, что и внешний интерфейс, необходимо убедиться в том, что у маршрутизатора восходящего потока есть статический маршрут к сопоставленной сети, который ведет к устройству защиты.

Устройство защиты записывает сеанс как выполненный и пересылает пакет из внешнего интерфейса. Если MAC-адрес назначения присутствует в таблице, устройство защиты передает пакет за пределы внешнего интерфейса. В качестве MAC-адрес назначения используется адрес маршрутизатора восходящего потока, 172.16.1.1. Если MAC-адрес назначения отсутствует в таблице устройства защиты, то устройство пытается его обнаружить при отправке запроса ARP и эхо-запроса. Первый пакет отбрасывается.

Сервер электронной почты отвечает на запрос. Поскольку сеанс уже выполняется, пакет не обходит множество поисков, связанных с новым соединением. Устройство защиты использует NAT для преобразования сопоставленного адреса в фактический адрес, 192.168.1.5.

Посещение внутреннего веб-сервера внутренним пользователем

Если узел A пытается получить доступ к внутреннему веб-серверу (10.1.1.1), то он (192.168.1.5) отправляет пакет запроса маршрутизатору Интернета (так как он используется в качестве шлюза по умолчанию) через ASA из внутренней среды во внешнюю. Пакет перенаправляется на веб-сервер (10.1.1.1) через ASA (из внешней среды во внутреннюю) и внутренний маршрутизатор.



Примечание. Пакет запроса возвращается на веб-сервер только в том случае, если список доступа ASA разрешает передачу трафика из внешней среды во внутреннюю.

Чтобы устранить эту проблему, необходимо назначить в качестве шлюза по умолчанию для узла A (10.1.1.1) внутренний маршрутизатор (192.168.1.3) вместо маршрутизатора Интернета (192.168.1.2). Это предотвращает передачу любого ненужного трафика на внешний шлюз, а если такой трафик появляется — перенаправляет его на внешний маршрутизатор (маршрутизатор Интернета). Он также производит обратное разрешение адресов, когда веб-сервер или любой другой узел, (10.1.1.0/24) представленный во внутренней среде внутреннего маршрутизатора, выполняет попытку доступа к узлу A (192.168.1.5).

Посещение внешним пользователем веб-сервера внутренней сети

Ниже приводится описание перемещения данных через устройство защиты.

Пользователь внешней сети выполняет запрос веб-страницы с внутреннего веб-сервера. Устройство защиты получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, система проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание. В многоконтекстном режиме устройство защиты вначале определяет пакет в соответствии с уникальным интерфейсом.

Устройство защиты вносит в журнал запись о созданном сеансе, только если внешнему пользователю разрешен доступ на внутренний веб-сервер. Доступ на веб сервер должен быть разрешен для внешнего пользователя с помощью списков доступа.

Если MAC-адрес назначения присутствует в таблице, устройство защиты передает пакет за пределы внутреннего интерфейса. В качестве MAC-адрес назначения используется адрес маршрутизатора нисходящего потока, 192.168.1.3.

Если MAC-адрес назначения отсутствует в таблице устройства защиты, то устройство пытается его обнаружить при отправке запроса ARP и эхо-запроса. Первый пакет отбрасывается.

Веб-сервер отвечает на запрос. Поскольку сеанс уже выполняется, пакет обходит множество поисков, связанных с новым соединением. Устройство защиты отправляет пакет внешнему пользователю.

Получение доступа для внешнего пользователя к внутреннему узлу

Пользователь внешней сети выполняет попытку доступа к внутреннему узлу. Устройство защиты получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, система проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание. В многоконтекстном режиме устройство защиты вначале определяет пакет в соответствии с уникальным интерфейсом.

Пакет отклоняется и устройство защиты отбрасывает его, поскольку у внешнего пользователя отсутствуют права доступа к внутреннему узлу. Если внешний пользователь предпринимает атаку на внутреннюю сеть, устройство защиты выполняет развертывание средств для определения, является ли пакет допустимым в уже выполняющемся сеансе.

Проверка

Используйте этот раздел для того, чтобы подтвердить, что ваша конфигурация работает правильно.

Средство Интерпретатор выходных данных (только для зарегистрированных клиентов) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра анализа выходных данных команды **show**.

```
ciscoasa(config)# sh firewall
Firewall mode: Transparent
```

Поиск и устранение неполадок

Сведения об устранении неполадок для этой конфигурации отсутствуют.

Дополнительные сведения

- **FWSM : Настройка прозрачного межсетевого экрана**
- **Устройства защиты (SA) Cisco серии PIX 500**
- **Устройства адаптивной защиты (ASA) Cisco серии 5500**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/100274/Transparent-firewall.shtml