Руководство по pfSense 2.0. Часть 9

Глава 9 Бриджинг (Мосты)

оглавление

Обычно, каждый интерфейс pfSense представляет собой свой широковещательный домен с уникальной IP подсетью, и действует так же как отдельный коммутатор. В некоторых случаях бывает желательно или необходимо объединить несколько интерфейсов в один широковещательный домен, где два порта брандмауэра будут действовать так, как будто они находятся на одном коммутаторе, за исключением трафика между интерфейсами, которым можно управлять с помощью правил брандмауэра. Обычно такой режим упоминается как прозрачный брандмауэр (transparent firewall).

9.1. Мосты и петли уровня 2 Используя мост, вы должны быть осторожны и избегать возникновения петель второго уровня, либо конфигурировать коммутатор для их обработки в соответствии с вашими требованиями. Петля второго уровня, создаёт тот же эффект, как если бы вы соединили кабелем два порта коммутатора. Если у вас присутствует развёртывание pfSense с двумя интерфейсами, эти интерфейсы объединены в мост, и оба интерфейса подключены к одному коммутатору, вы создали петлю уровня 2. Соединение двух коммутаторов двумя патч-кордами приведёт к тому же эффекту. Управляемые коммутаторы используют протокол Spanning Tree Protocol (STP) для обработки подобной ситуации, поскольку часто бывает необходимо иметь несколько связей между коммутаторами, а вы явно не желаете, чтобы ваша сеть упала если кто-то подключит один порт в другой. STP не включается по умолчанию на всех управляемых коммутаторах, и почти никогда не доступен на неуправляемых коммутаторах. При отсутствии STP, кадры в петле уровня 2 попадают в замкнутый цикл, а сеть перестаёт функционировать до тех пор, пока цикл не будет удалён. В двух словах - мост имеет потенциал полностью вывести из строя сеть если вы не понимаете что делаете.

9.2. Мосты и брандмауэры Фильтрация с функциями объединения интерфейсов не отличается от маршрутизируемых интерфейсов. правила брандмауэра применяются на каждом участвующем интерфейсе моста на входящей основе. Те, кто некоторое время использует pfSense, могут вспомнить о включении флага Enable filtering bridge, на странице System -> Advanced. Ссылки на данный флаг являются устаревшей информацией. Она была унаследована из m0n0wall, который реализовал мост иным способом. В pfSense используются различные способы

преодоления необходимости данного флага, а пути построения моста в новых версиях FreeBSD не позволяют работать с не фильтрующим мостом пока вы полностью не

Автор: 02.04.12 14:54 - Последнее обновление 02.04.12 15:24

отключите pf.

9.3. Мост двух внутренних сетей Вы можете объединить две внутренние сети для создания одного широковещательного домена и включить фильтрацию трафика между двумя интерфейсами. Обычно, это делается с беспроводным интерфейсом, сконфигурированным как точка доступа, для соединения проводных и беспроводных сегментов в одном широковещательном домене.

Иногда, брандмауэр с интерфейсами LAN и OPT может использоваться в качестве коммутатора, в сетях, где необходимы только две внутренних системы. Вы можете столкнуться и со сценариями, в которых два интерфейса брандмауэра должны находится в одном широковещательном домене для каких-то других специфических целей.

Замечание Существуют дополнительные требования и ограничения, когда объединяются беспроводные интерфейсы, что связано со способом функционирования 802.11. Смотрите раздел 18.3, "Мосты и беспроводные сети" для получения дополнительной информации.

9.3.1. DHCP и внутренние мосты Если вы объединяете одну внутреннюю сеть с другой, необходимо сделать две вещи. Прежде всего убедитесь, что DHCP работает только на основном интерфейсе (с IP адресом), а не на одном из подключаемых в мост. Во-вторых, вам понадобится дополнительное правило брандмауэра вверху набора правил для данного OPT интерфейса, разрешающее DHCP-трафик. Как правило, при создании правила разрешающего трафик на интерфейсе, источник (source) указывается аналогично "OPT1 Subnet", так, что только трафику от подсети разрешается покидать данный сегмент. При использовании DHCP этого не достаточно. Поскольку клиент ещё не имеет IP адреса, DHCP запрос выступает как широковещательный. Для удовлетворения этих запросов, вам необходимо создать правило на интерфейсе моста с Protocol установленным в UDP, Source установленным в 0.0.0.0 и портом источника 68, Destination установленным в 255.255.255.255, и портом назначения 67. Добавьте описание, похожее на "Allow DHCP", а затем нажмите кнопку Save и Apply Changes. В итоге, вы получите правило которое выглядит так как показано на рисунке 9.1, "Правило брандмауэра для разрешения DHCP".

www.thin.kiev.ua - Руководство по pfSense 2.0. Глава 9 Бриджинг (Мосты)

Автор: 02.04.12 14:54 - Последнее обновление 02.04.12 15:24

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
3 0	LIDP	0.0.0.0	68	255.255.255.255	67	.*		Allow DHCP
		LAN net	+	•	•	•		Default LAN ne Any
<u>Geb</u>					in na Dki		the second detailed	
								AVP
		er craimisolo	ridgeoberk		m/mina/	hond the second		eac. Dear
			BRIDE BRIDE STATE AND		,			
	말한말한만난단?				<u>e uvioille</u>	со элемента	ПОЗВОЛИТ	
1				HEEMAHHHHHHAD OT	enviouie n	со элемента Сортемента		p pę
1-10-14				la taxa human takan walan kan kan kan kan kan kan kan kan kan k				npe Note
1-19.14								
	wan w	LAN		ia in the second s				
	wan w	LAN						n pę Novia K
	wan w Proto	LAN Source	Port	Destination	e ny jour n Port	Gateway	Schedule	Description
	WAN W Proto	LAN	Port	Destination	Port	Gateway	Schedule	Description
	WAN W Proto	LAN Source 0.0.0.0	Port 68	Destination 255.255.255.255	Port 67	Gateway	Schedule	Description Allow DHCP
	WAN W Proto	LAN Source 0.0.0.0	Port 68	Destination 255.255.255.255	Port 67	Gateway	Schedule	Description
5 5 7	WAN W Proto UDP	LAN C.O.O.O	Port 68	Destination 255.255.255.255	Port 67	Gateway *	Schedule	Description Allow DHCP
	WAN W Proto UCP	LAN COLOR	Port 58	Destination 255.255.255.255	Port 67	Gateway	Schedule	Description Allow DHCP Default LAN ne
	WAN W Proto UDP	LAN Source 0.0.0.0 LAN net	Port 58 +	Destination 255.255.255.255 *	Port 67	Gateway *	Schedule	Description Allow DHCP Default LAN no Any
	WAN W Proto UDP	LAN Source 0.0.0.0 LAN net	Port 68 +	Destination 255.255.255.255 *	Port 67	Gateway *	Schedule	Description Allow DHCP Default LAN ne Any
	WAN W Proto	LAN Source 0.0.0.0 LAN net	Port 58 +	Destination 255.255.255 *	Port 67	Gateway *	Schedule	Description Allow DHCP Default LAN ne Any