SMART-SOFT

НАСТРОЙКА РАЗРЕШАЮЩИХ ФИЛЬТРОВ ДЛЯ ГРУППЫ, ГДЕ ВСЕ ЗАПРЕЩЕНО

Чтобы жестко ограничить доступ к сети интернет какой-то группе пользователей:

1. Создайте группу с фильтром на запрещение. Для этого при создании группы на вкладке «Фильтрация» установите галку «Блокировать весь трафик по умолчанию».

Новая группа ? х					
Новая груг Новая груг Наименование Авторизация Настройки агентов Автодобавление Тарификация Расписание Сетевая статистика Сетевая статистика Контроль нарушений Фильтрация Правила группы "До"	Новая группа па Блокировка всего трафика по умолчанию Использовать общие настройки Э Блокировать весь трафик по умолчанию	?	×		
 П перенаправление ТСР Ограничения Шейпер Автоматизация Запись в журнал Создать группу 	■ Блокировать весь трафик по умолчанию при работе в кредит < Назад	мена			

2. Создайте фильтр на разрешение (в примере создается фильтр на разрешение SMTP по 25 порту).

	Новое правило ? Х					
Новое правило						
 Наименование Тип трафика Тип правила IP адрес IP протокол Расширенная фильтр Дополнительно Расписание Тарификация Шейпер Роутинг Сохранить данные Готово 	Имя SMTP введите уникальное имя Запретить правило Описание					
Помощь Новое пра	<назад Далее > Отмена Новое правило ? х авило					
 Наименование Тип трафика Тип правила ПР адрес ІР протокол Расширенная фильтр Дополнительно Расписание Тарификация Шейпер Роутинг Сохранить данные Готово 	 Разрешение + "действия" Комбинированное правило - кроме разрешения данного трафика также описываются различные другие действия. Запрет Трафик, подпадающий под заданное условие, будет заблокирован. Для трафика через НТТР прокси возможно задание дополнительных действий. Управляемое пользователем Имеет смысл, если данное правило применено для пользователя. задайте уровень правила (F1-F4). Баннеры Тользователь сам задает свой уровень фильтрации. Правило применяется, если уровень правила (F1-F4) не более уровня пользователя. Только "действия" 					
Помощь	< Назад Далее > Отмена					

В поле «порт назначения» вписываются порты удаленного сервера, в нашем примере это 25 порт, стандартный для почты (SMTP). Можете выбрать протокол из списка шаблонов.

	Новое правило	? X
Новое пр	авило	
 Наименование Тип трафика Тип правила IP адрес IP протокол Расширенная фильтр Дополнительно Расписание Тарификация Шейпер Роутинг Сохранить данные Готово 	Подсказка - выберите протокол из списка шаблонов SMTP client (TCP/25) V Протокол TCP V Тип (номер) IP протокола 6 (1-255) TCP/UDP порты источника • Порт / диапазон портов • Динамические порты 25 • • • • • • Динамические порты	
Помощь	< Назад Далее > Отме	ена
И Новое пр	Новое правило	? X
Корональский в положит положит Положит положит положи Потово положит положит Положит положит положит Положит положит положит Положит положит положит положит положит положит положит положит положит положит пол	Новое правило авило Новое описание правила создано. Создать еще Этот мастер будет вызван повторно.	? ×

Примените данное правило к группе пользователей. Это делается в свойствах группы.

	Настройка группы	? X				
Настройн	а группы					
Наименование Авторизация Настройки агентов Автодобавление Тарификация Расписание Сетевая статистика	 Правила "До" - по умолчанию Эти правила действуют на всю группу до индивиду которые назначены на пользователей. Правила группы "До" Выберите описание группы правил и нажмите "Доба 	уальных правил, авить" Добавить				
Контроль нарушений	Выберите описание правила и нажмите "Добавить"					
Правила группы "До"	SMTP	Добавить				
Правила группы "После" НТТР мимо прокси Перенаправление ТСР Ограничения Шейпер Автоматизация Запись в журнал	Agent> rpynna SMTP paspe	Вверх				
Помощь	ОК	Удалить				

Обратите внимание, что для полноценной работы почты надо добавить еще 2 фильтра на разрешение по портам 110 и 143.

Подобным образом можно сделать и наоборот - запретить только почту (соответственно при создании группы не нужно устанавливать галку «Блокировать весь трафик по умолчанию» и фильтры надо создавать на запрещение).

Соответственно можно создать несколько групп с разными запрещающими или разрешающими фильтрами, которые будут действовать только на пользователей данной группы.

Приложение

Таблица наиболее часто используемых протоколов

Название	Протокол	транспортный протокол	Порт	Примечание
Почта	SMTP	ТСР	25	В этих фильтрах можно еще добавить им
	POP3	ТСР	110	что если DNS внешний, то необходимо открыть
	IMAP	ТСР	143	еще порты DNS см.таб.
DNS		UDP	53	
DHCP		UDP	67	
		UDP	68	
FTP	FTP- DATA	ТСР	20	
	FTP	ТСР	21	
WWW		ТСР	80	
Proxy (TI)	HTTP	ТСР	8080	
	Socks	ТСР	1080	
ICQ IP сети			Приме	ечание
	205.188.0.0/255.255.0.0		ICQ r	работает с разными портами, поэтому лучше
	64.12.0.0/255.255.0.0		разрешать диапазон сетей.	

Для настройки фильтров по другим протоколам, если не знаете порт и тип транспортного протокола, воспользуйтесь сетевой статистикой в программе.