

Настройка межсетевого экрана

Задание:

1. Сервера и Администраторы офиса DT должны иметь доступ ко всем устройствам
2. Клиенты офиса DT должны иметь доступ только к серверам
3. Разрешите ICMP-запросы администраторами офиса DT на внутренние интерфейсы межсетевого экрана

Вариант реализации:

ADMIN-DT:

- Поскольку всё что не запрещено явно, то разрешено, для выполнения данного блока достаточно следующего набора правил для FORWARD:
 - Сервера и Администраторы офиса DT должны иметь доступ ко всем устройствам - имеют;
 - Клиенты офиса DT должны иметь доступ только к серверам - имеют, всё остальное запрещено;
 - Разрешите ICMP-запросы администраторами офиса DT на внутренние интерфейсы межсетевого экрана - имеют

Протокол	Зона	Адрес	Порты	НП...	Зона	Адрес	Порты	Действие	Про...	Комментарий	Управление
* Любой	v110	Clients DT	* Любой	-	v120	Servers DT	* Любой	Разрешить	-	Доступ для клиентов DT к серверам DT	🟢 + - 1
* Любой	v110	Clients DT	* Любой	-	* Любой	Servers HQ	* Любой	Разрешить	-	Доступ для клиентов DT к серверам HQ	🟢 + - 1
* Любой	v110	Clients DT	* Любой	-	* Любой	* Любой	* Любой	Запретить	-	Запрет доступа клиентам DT	🟢 + - 1

- Или же реализация принципа "всё что не разрешено, то запрещено":
 - FORWARD:

Протокол	Зона	Адрес	Порты	НП...	Зона	Адрес	Порты	Действие	Про...	Комментарий	Управление
* Любой	v120	Servers DT	* Любой	-	* Любой	* Любой	* Любой	Разрешить	-	Сервера DT доступ ко всем устройствам	🟢 + - 1
* Любой	v1330	Administrators DT	* Любой	-	* Любой	* Любой	* Любой	Разрешить	-	Администраторы DT доступ ко всем устройствам	🟢 + - 1
* Любой	v110	Clients DT	* Любой	-	v120	Servers DT	* Любой	Разрешить	-	Клиенты DT доступ к серверам DT	🟢 + - 1
* Любой	v110	Clients DT	* Любой	-	* Любой	Servers HQ	* Любой	Разрешить	-	Клиенты DT доступ к серверам HQ	🟢 + - 1
* Любой	* Любой	* Любой	* Любой	-	* Любой	* Любой	* Любой	Запретить	-	Запрет всего остального	🟢 + - 1

◦ INPUT:

Протокол	Зона	Адрес	Порты	НП...	Зона	Адрес	Порты	Действие	Про...	Комментарий	Управление
TCP	v1330	Administrators DT	* Любой	-	v1330	FW-DT WEB		Разрешить	-	Для доступа к веб-интерфейсу FW-DT из v1330	🟢 + - 1
ICMP	v1330	Administrators DT	* Любой	-	v110, v120, v1330	FW-DT - R-DT		Разрешить	-	Для ICMP-запросов из v1330 на внутренние интерфейсы FW-DT	🟢 + - 1
* Люб...	* Люб...	* Люб...	* Люб...	-	* Люб...	* Люб...	* Люб...	Запретить	-	Запрет всего остального	🟢 + - 1

Последнее изменение: среда, 25 декабря 2024, 11:04

Обратная связь

Подпишитесь

Вы используете гостевой доступ (Вход)

Сводка хранения данных

Тема оформления сайта разработана

