

## Межсетевой экран ССПТ-2. Фильтрация.

Межсетевой экран ССПТ-2 обеспечивает фильтрацию трафика в невидимом режиме работы (отсутствие адресов на фильтрующих интерфейсах) на следующих уровнях:

### 1. Канальный уровень

Обеспечивается фильтрация на основании анализа заголовков следующих типов кадров:

- Ethernet II/DIX;
- IEEE 802.3/LLC;
- IEEE 802.3-SNAP;
- IEEE 802.3 Raw;
- IEEE 802.1p/q.

Для принятия решения о действии, производимом над кадром (пропуск, передача, удаление) используются адресные поля заголовка (адрес отправителя и адрес получателя), а так же поле типа вложенного протокола.

Поддержка виртуальных локальных сетей (VLAN) стандарта IEEE 802.1p/Q обеспечивает возможность построения индивидуальной политики безопасности для каждой виртуальной локальной сети.

### 2. Межсетевой уровень

Обеспечивается фильтрация протоколов IP4 и IPX.

При фильтрации протокола IP используется информация следующих полей заголовка:

- IP адрес отправителя;
- IP адрес получателя;
- Номер протокола транспортного уровня;
- Флаг precedence;
- Флаги TOS;
- Флаги фрагментации пакета;
- Поле максимальной длины пакета;
- TTL.

При задании IP-адресов возможно задание определенного адреса, адреса подсети, а так же перечисления адресов или подсетей.

При фильтрации протокола IPX используется информация следующих полей заголовка:

- Тип пакета;
- Адрес сети отправителя;
- Адрес узла отправителя;
- Адрес сети получателя;
- Адрес узла получателя;
- Номер сокета отправителя;
- Номер сокета получателя.

### **3. Транспортный уровень**

Обеспечивается фильтрация на основании анализа заголовков пакетов для протоколов UDP и TCP. При этом используется информация полей номера порта отправителя и номера порта получателя пакета, а для протокола TCP так же анализируются флаги контроля сессии.

### **4. Прикладной уровень**

Обеспечивается фильтрация следующих протоколов прикладного уровня: HTTP (адреса и фрагменты URL), SMTP, POP3 (почтовые адреса отправителя и получателя), FTP (идентификатор и пароль пользователя, расширения перекачиваемых файлов), протоколы SQL (SQL\*Net, MS-SQL, Potgresql, Mysql – sql-запросы и их фрагменты), DNS (доменные имена) и другие прикладные протоколы (фильтрация по любому фрагменту заголовка прикладного уровня).

### **5. Дополнительно**

Обеспечивается фильтрация следующих протоколов, вложенных в Ethernet-кадр: IPv4, IPv6, IPX, ARP/RARP и других протоколов в соответствии со значением соответствующего поля в заголовке Ethernet-кадра.

**Поддержка механизма управления сессиями.** Обеспечивается контроль корректности переходов между состояниями виртуального соединения TCP в соответствии с флагами управления, а так же контроль корректности номеров последовательностей.