Руководство пользователя по эксплуатации

версия 1 ред. от 30.05.2024

Листов 48

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. Таблица «Термины и сокращения»).

Таблица «Термины и сокращения»

Термины и сокращения	Значение
ИБ	Информационная безопасность
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
ЦП	Центральный процессор
ARMA Стена	ARMA InfoWatch Стена
CA	Certification authority – центр сертификации
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
FTP	File Transfer Protocol – протокол передачи файлов по сети
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
LAN	Local Area Network – локальная вычислительная сеть
NAT	Network Address Translation, преобразование сетевых адресов – технология преобразования IP-адресов
NTLMv2	NT LAN Manager – протокол сетевой аутентификации, встроенный в ОС Microsoft Windows

Термины и сокращения	Значение
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
RFC	Request for Comments, рабочее предложение – документ из серии пронумерованных информационных документов Интернета
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDPB
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	Secure Sockets Layer, уровень защищённых сокетов – криптографический протокол
STP	Spanning Tree Protocol, протокол остовного дерева – канальный протокол, предназначенный для устранения петель в топологии сети Ethernet
SYN cookie	Техника противодействия SYN-флуд-атаке
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
TLS	Transport layer security – протокол защиты транспортного уровня
USB	Universal Serial Bus – универсальная последовательная шина
UUCP	Unix-to-unix copy – команда копирования файлов между двумя компьютерами под управлением операционной системы UNIX, использующая одноимённый протокол
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих

Термины и сокращения	Значение
	обеспечить одно или несколько сетевых соединений поверх другой сети
VRRP	Virtual Router Redundancy Protocol, протокол резервирования виртуального маршрутизатора – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
WAN	Wide Area Network – глобальная вычислительная сеть

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **InfoWatch ARMA Стена v.4.2**.

Руководство пользователя по эксплуатации описывает принципы работы с **ARMA Стена**, доступные функции, их подробное описание, настройку и использование.

Пользователю **ARMA Стена** необходимо изучить настоящее руководство перед эксплуатацией.

1 МЕЖСЕТЕВОЙ ЭКРАН

Одной из основных функций **ARMA Стена** является фильтрация трафика с помощью встроенного межсетевого экрана.

1.1 Правила МЭ

1.1.1 Глобальные настройки

Для просмотра конфигурации МЭ необходимо ввести команду **«show firewall»**.

Правилами МЭ предусмотрены следующие действия над пакетами:

- **«accept»** – разрешить;
- **«drop»** – блокировать;
- **«reject»** – отклонить.

Возможно применение вышеперечисленных действий над следующими категориями пакетов:

- **«established»** – для установленного соединения;
- **«invalid»** – недопустимых пакетов;
- **«related»** – для связанных соединений.

Пример правила:

```
set firewall state-policy invalid action drop
```

Возможно включение/отключение следующих опций:

1. Отправление **ARMA Стена** ответов на локальные ICMP-запросы:

   ```
   set firewall all-ping enable/disable
   ```

   Включено по умолчанию.

2. Отправление **ARMA Стена** ответов на широковещательные ICMP-запросы:

   ```
   set firewall broadcast-ping enable/disable
   ```

3. Использование **ARMA Стена** «SYN cookie»:

   ```
   set firewall syn-cookies enable/disable
   ```

Для копирования правила МЭ с целью последующего его редактирования следует ввести следующие команды:

```
[edit]
admin@ngfwos# edit firewall name ALL
[edit firewall name ALL]
admin@ngfwos# copy rule 21 to rule 31
```

где «ALL» – имя набора правил; «21» – идентификатор копируемого правила; «31» – идентификатор копии правила. Приведены в качестве примера.

Для переименования правила МЭ следует ввести следующие команды:

```
[edit]
admin@ngfwos# edit firewall name ALL
[edit firewall name ALL]
admin@ngfwos# rename rule 11 to rule 15
```

где «ALL» – имя набора правил; «11» – изначальный идентификатор правила; «15» – идентификатор переименованного правила. Приведены в качестве примера.

1.1.2 Журналирование

Для включения журналирования следует использовать следующие команды:

```
set firewall state-policy established log enable
set firewall state-policy invalid log enable
set firewall state-policy related log enable
```

1.1.3 Наборы правил МЭ

Наборы правил МЭ необходимо предварительно создавать для последующего добавления в них правил МЭ.

Для создания набора правил МЭ необходимо ввести следующую команду:

```
set firewall name Local1 description LAN1
```

где «Local1» – имя набора правил; «LAN1» – описание.

Для назначения действия по умолчанию для набора правил в случае, если ни одно из установленных правил в наборе не было применено необходимо ввести следующую команду:

```
set firewall name Local1 default-action drop
```

где «drop» – действие по умолчанию. Приведено в качестве примера.

Для включения журналирования действий по умолчанию необходимо ввести следующую команду:

```
set firewall name Local1 enable-default-log
```

Для добавления правила в набор и указания действия необходимо ввести следующую команду:

```
set firewall name Local1 rule 10 action accept
```

где «10» – идентификатор правила, может принимать значение в диапазоне от «1» до «999999»; «accept» – действие. Приведено в качестве примера.

Для добавления описания правила МЭ необходимо ввести следующую команду:

```
set firewall name Local1 rule 10 description Text
```

где «Text» – описание.

Для включения журналирования по определённому правилу необходимо ввести следующую команду:

```
set firewall name Local1 rule 10 log enable
```

где «enable» – включение.

Для отключения правила МЭ необходимо ввести следующую команду:

```
set firewall name Local1 rule 10 disable
```

где «disable» – отключение.

1.1.4 Пример создания правила для группы IP-адресов

В качестве примера приведён список команд для создания блокирующего правила, отклоняющего пакеты от адресатов в указанном диапазоне:

```
set firewall group address-group BLOCK address 192.168.56.100-192.168.56.200
set firewall name ALL rule 10 action reject
set firewall name ALL rule 10 source group address-group BLOCK
set interfaces ethernet eth0 firewall local name ALL
```

где «BLOCK» – имя группы IP-адресов; «192.168.56.100-192.168.56.200» – диапазон IP-адресов; «ALL» – имя набора правил.

1.1.5 Группы сетей

ARMA Стена поддерживает объединение сетей в группу с помощью ввода следующих команд:

```
set firewall group network-group inside-v4 network 192.168.21.0/24
set firewall group network-group inside-v4 network 192.168.25.68/32
```

где «inside-v4» – имя группы сетей; «192.168.21.0/24» – адрес сети в формате CIDR; «192.168.25.68/32» – IP-адрес хоста. Приведено в качестве примера.

1.1.6 Группы портов

ARMA Стена поддерживает объединение портов в группу с помощью ввода следующих команд:

```
set firewall group port-group server1-port-TCP port 443
set firewall group port-group server1-port-TCP port 507-512
```

где «server1-port-TCP» – имя группы портов; «443» – номер порта; «507-512» – диапазон портов, граничные значения диапазона разделяются символом «-». Приведено в качестве примера.

1.2 Политика на основе зон

В политике на основе зон интерфейсы назначаются зонам, а фильтрация применяется к трафику между зонами и обрабатывается в соответствии с правилами МЭ.

Основные тезисы:

- зона должна быть сконфигурирована до того, как ей будет назначен интерфейс, а интерфейс может быть назначен только одной зоне;
- разрешён весь входящий и исходящий трафик интерфейса в пределах зоны;
- весь трафик между зонами зависит от существующих политик;
- трафик не может передаваться между интерфейсом-участником зоны и любым интерфейсом, который не является участником этой зоны;
- необходима настройка отдельных МЭ, по одному для каждого направления трафика.

В качестве примера приведён список команд для разрешения доступа из локальной сети в сеть Интернет:

```
set zone-policy zone LAN local-zone
set zone-policy zone WAN interface eth0
set firewall name allow rule 10 action accept
set firewall name allow default-action accept
set zone-policy zone LAN from WAN firewall name allow
set zone-policy zone WAN from LAN firewall name allow
```

где «LAN» и «WAN» – имена зон; «eth0» – интерфейс с доступом к сети Интернет; «allow» – имя набора правил.

2 NAT

Трансляция сетевых адресов, сокращённо NAT – это технология преобразования IP-адресов внутренней сети «LAN» в IP-адреса внешней сети «WAN».

2.1 Правила NAT

С помощью правил NAT возможно осуществлять фильтрацию трафика, применяя следующие фильтры:

1. **«outbound-interface»** – для интерфейсов, используемых для внешнего трафика:

```
set nat source rule 11 outbound-interface eth0
```

2. **«inbound-interface»** – для интерфейсов, используемых для внутреннего трафика:

```
set nat destination rule 21 inbound-interface eth1
```

3. **«protocol»** – для трансляции пакетов, соответствующих указанным протоколам:

```
set nat source rule 11 protocol tcp_udp
```

   где «11» – идентификатор правила, «tcp_udp» – протоколы «tcp» и «udp», разделяемые в списке символом «_».

   По умолчанию правило относится ко всем протоколам.

4. **«source»** – для указания адреса источника и прослушиваемого порта:

```
set nat source rule 22 source address 198.51.100.0/24
set nat source rule 22 source port 80,443
```

   где «198.51.100.0/24» – адрес сети; «80,443» – номера портов «80» и «443», разделяемые в списке символом «**,**».

5. **«destination»** – для указания адреса назначения:

```
set nat source rule 33 destination address 192.168.1.2
```

Для правил SNAT адрес источника пакетов будет заменён адресом, указанным в команде «translation»:

```
set nat source rule 44 translation address masquerade
```

Для просмотра конфигурации NAT необходимо ввести команду **«show nat»**.

2.2 Примеры создания правил NAT

2.2.1 NAT

В качестве примера приведён список команд для создания правила NAT, преобразующего адрес источника:

```
set nat source rule 11 outbound-interface eth0
set nat source rule 11 source address 192.168.43.0/24
set nat source rule 11 translation address masquerade
```

где «eth0» – интерфейс с доступом к сети Интернет, «192.168.43.0/24» – адрес сети LAN в формате CIDR.

2.2.2 NAT «Переадресация портов»

В качестве примера приведён список команд для создания правила NAT «Переадресация портов», перенаправляющего на внутренний веб-сервер с IP-адресом «192.168.3.112» HTTP-трафик по протоколу «TCP» через порт «80»:

```
set nat destination rule 21 description 'Port Forward: HTTP to 192.168.3.112'
set nat destination rule 21 destination port 80
set nat destination rule 21 inbound-interface eth0
set nat destination rule 21 protocol tcp
set nat destination rule 21 translation address 192.168.3.112
```

2.2.3 NAT «один-к-одному»

Статический NAT «Один-к-одному» сопоставляет один внешний IP-адрес, в большинстве случаев общедоступный, с одним внутренним IP-адресом, в большинстве случаев частным.

В качестве примера приведён **ARMA Стена**, сетевые интерфейсы которого настроены следующим образом:

```
[edit]
admin@ngfwos# show interfaces
 ethernet eth0 {
        address 203.0.113.87/24
        description WAN
        hw-id 00:50:56:bd:ca:9e
 }
 ethernet eth1 {
        address 192.168.2.1/24
        description LAN
        hw-id 00:50:56:bd:f5:cd
 }
 loopback lo {
 }
```

Для создания правила NAT «один-к-одному» следует ввести следующие команды:

```
set nat destination rule 31 description '1-to-1 NAT example'
set nat destination rule 31 destination address 203.0.113.87
set nat destination rule 31 inbound-interface eth0
set nat destination rule 31 translation address 192.168.2.10
set nat source rule 31 description '1-to-1 NAT example'
set nat source rule 31 outbound-interface eth0
set nat source rule 31 source address 192.168.2.10
set nat source rule 31 translation address 203.0.113.87
```

3 СЕТЕВЫЕ ИНТЕРФЕЙСЫ

Просмотр конфигурации интерфейсов возможен с помощью команды **«show interfaces»**. В случае запроса конфигурации интерфейсов в режиме конфигурирования дополнительно будет отображена информация о MAC-адресах.

Интерфейсам по умолчанию назначается имя «ethN», где «N» – идентификатор, присвоенный интерфейсу системой.

Используемые далее имена интерфейсов и IP-адреса приведены в качестве примера и могут отличаться для каждой конкретной ситуации.

3.1 Назначение IP-адреса

Для назначения IP-адреса на интерфейсе необходимо ввести команду:

```
set interfaces ethernet eth1 address 192.168.67.1/24
```

где «eth1» – имя интерфейса, «192.168.67.1/24» – IP-адрес в формате CIDR.

Возможно назначение нескольких IP-адресов на интерфейсе. Каждый указанный IP-адрес не заменяет назначенный ранее.

Для добавления описания интерфейса следует ввести команду:

```
set interfaces ethernet eth1 description 'LAN'
```

где «LAN» – описание.

Пример вывода информации о настроенных интерфейсах:

```
[edit]
admin@ngfwos# show interfaces
Must specify config path
 ethernet eth0 {
        address dhcp
        description WAN
        hw-id 00:50:56:bd:f5:cd
 }
 ethernet eth1 {
        address 192.168.67.1/24
        address 192.168.67.2/24
        description LAN
        hw-id 00:50:56:bd:ca:9e
 }
 loopback lo {
 }
```

При необходимости получения IPv4-адреса по протоколу «DHCP» на интерфейсе следует ввести команду:

```
set interfaces ethernet eth0 address dhcp
```

При необходимости получения IPv6-адреса по протоколу «DHCP» на интерфейсе следует ввести команду:

```
set interfaces ethernet eth0 address dhcpv6
```

Для назначения MAC-адреса для интерфейса следует ввести команду:

```
set interfaces ethernet eth2 mac 00:11:22:33:44:55
```

Для создания VLAN-интерфейса следует ввести команду:

```
set interfaces ethernet eth1 vif 2
```

где «2» – идентификатор VLAN. Возможно использовать значения в диапазоне от «0» до «4094».

Для включения прокси ARP для интерфейса следует ввести команду:

```
set interfaces ethernet eth1 ip enable-proxy-arp
```

4 СЕТЕВОЙ МОСТ

Сетевой мост – это объединение различных сегментов сети передачи данных в единую сеть.

Для создания сетевого моста необходимо выполнить следующие действия:

1. Для включения функции «STP» следует ввести команду:

```
set interfaces bridge br0 stp
```

   где «br0» – имя сетевого интерфейса.

2. Для добавления интерфейсов-участников моста «br0» следует ввести следующие команды:

```
set interfaces bridge br0 member interface eth0
set interfaces bridge br0 member interface eth1
```

3. Для назначения MAC-адреса для моста «br0» следует ввести команду:

```
set interfaces bridge br0 mac 00:11:11:00:22:22
```

   где «00:11:11:00:22:22» – MAC-адрес.

Возможно добавление описания с помощью ввода следующей команды:

```
set interfaces bridge br0 description Bridge0
```

где «Bridge0» – описание.

Для отключения моста следует ввести команду:

```
set interfaces bridge br0 disable
```

5 МАРШРУТИЗАЦИЯ

5.1 Настройка шлюза по умолчанию

Для настройки шлюза по умолчанию необходимо ввести следующую команду:

```
set protocols static route 0.0.0.0/0 next-hop 172.16.2.1
```

где «172.16.2.1» – IP-адрес. Приведён в качестве примера.

Для удаления шлюза по умолчанию необходимо ввести следующую команду:

```
delete protocols static route 0.0.0.0/0
```

Для просмотра информации о маршруте по умолчанию необходимо ввести команду **«show ip route 0.0.0.0»**:

```
admin@ngfwos:~$ show ip route 0.0.0.0
```

5.2 Настройка статического маршрута

Для настройки статического маршрута необходимо ввести следующую команду:

```
set protocols static route 172.16.32.0/24 next-hop 172.16.32.1
```

где «172.16.32.0/24» – адрес сети, «172.16.32.1» – IP-адрес.

Возможно указание нескольких статических маршрутов.

Для указания дистанции для маршрута необходимо ввести следующую команду:

```
set protocols static route 172.16.32.0/24 next-hop 172.16.32.1 distance 10
```

где «10» – значение дистанции. Приведено в качестве примера. Возможно указание значения в диапазоне от «1» до «255». Маршрут с назначенным значением дистанции «1» будет иметь наивысший приоритет.

По умолчанию используется значение «1».

Для отключения статического маршрута необходимо ввести следующую команду:

```
set protocols static route 172.16.32.0/24 next-hop 172.16.32.1 disable
```

5.3 VRF

VRF – технология, позволяющая в пределах одного маршрутизатора создавать несколько таблиц маршрутизации одновременно.

В качестве примера на **ARMA Стена** для интерфейса «eth1» назначен IP-адрес – «10.0.0.1/24».

Для создания виртуального маршрутизатора необходимо ввести следующие команды:

```
set vrf name vrf1 table 100
set interfaces ethernet eth1 vrf vrf1
```

где «vrf1» – имя VRF, «ethernet» – тип интерфейса, «100» – идентификатор таблицы маршрутизации.

Примечание:

Изменение идентификатора таблицы маршрутизации возможно только, если удалить его и задать новое значение.

Для просмотра таблицы маршрутизации следует ввести следующие команды.

```
admin@ngfwos:~$ show ip route
```

Интерфейс «eth1» будет отсутствовать в данной таблице.

```
admin@ngfwos:~$ show ip route vrf vrf1
```

Интерфейс «eth1» будет отображаться в данной таблице.

6 НАСТРОЙКА ОТКАЗОУСТРОЙЧИВОГО КЛАСТЕРА

В режиме отказоустойчивого кластера несколько **ARMA Стена** объединяются в единый кластер в режиме «active-backup».

В случае объединения нескольких **ARMA Стена** в каждый момент времени только одно устройство **ARMA Стена** в кластере обрабатывает весь трафик, такое устройство считается ведущим. При выходе из строя ведущего устройства его подменяет одно из резервных устройств, которое само становится ведущим и начинает обрабатывать трафик. В случае если изначально ведущее устройство вновь переходит в рабочее состояние, то текущее ведущее устройство возвращается в статус подчинённого резервного устройства.

Данный подход реализуется с помощью протокола VRRP, предназначенного для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию.

6.1 Настройка устройств кластера

Для настройки работы **ARMA Стена** в режиме отказоустойчивого кластера используется схема, представленная на рисунке (см. Рисунок – Схема стенда для настройки режима отказоустойчивого кластера).

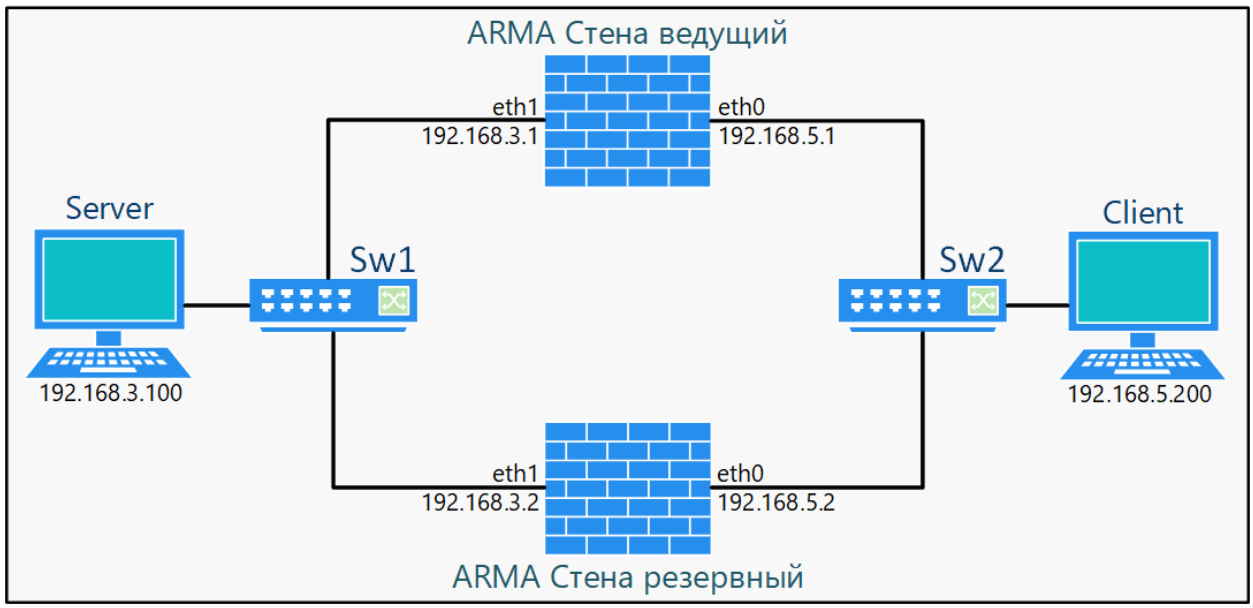

Рисунок – Схема стенда для настройки режима отказоустойчивого кластера

Для настройки работы в режиме отказоустойчивого кластера и создания виртуального маршрутизатора в сети «192.168.3.0/24» на каждом **ARMA Стена** необходимо выполнить следующие действия:

1. Назначить имя виртуального маршрутизатора и перейти к его настройке:

```
[edit]
admin@ngfwos# set high-availability vrrp group gr1
[edit]
admin@ngfwos# edit high-availability vrrp group gr1
[edit high-availability vrrp group gr1]
admin@ngfwos#
```

где «gr1» – имя виртуального маршрутизатора.

2. Назначить интерфейс:

```
[edit high-availability vrrp group gr1]
admin@ngfwos# set interface eth1
```

где «eth1» – имя интерфейса.

3. Назначить идентификатор:

```
[edit high-availability vrrp group gr1]
admin@ngfwos# set vrid 50
```

где «50» – идентификатор.

4. Назначить виртуальный адрес:

```
[edit high-availability vrrp group gr1]
admin@ngfwos# set virtual-address 192.168.3.254/24
```

где «192.168.3.254/24» – виртуальный IP-адрес в формате CIDR.

5. Указать приоритет для виртуального маршрутизатора:

```
[edit high-availability vrrp group gr1]
admin@ngfwos# set priority 200
```

где «200» – величина приоритета. Возможно указать значение в диапазоне от «1» до «255». Значение «255» соответствует наивысшему приоритету. По умолчанию используется значение «100».

Для просмотра статуса необходимо ввести команду **«show vrrp»**:

```
admin@ngfwos:~$ show vrrp
```

Для отключения виртуального маршрутизатора следует ввести команду:

```
[edit]
admin@ngfwos# set high-availability vrrp group gr1 disable
```

7 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Функциональность системы обнаружения и предотвращения вторжений в **ARMA Стена** реализуется посредством ПО с открытым исходным кодом «Suricata» и использованием метода захвата пакетов «Netmap» для повышения производительности и минимизации загрузки ЦП.

7.1 Основные настройки СОВ

Включение и выключение какого-либо параметра СОВ осуществляется с помощью атрибутов «yes» и «no» соответственно.

Для включения СОВ необходимо ввести следующую команду:

```
set suricata enable yes
```

Для включения журналирования СОВ необходимо ввести следующую команду:

```
set suricata stats enabled yes
```

Для включения записи уведомлений срабатываемых событий СОВ в файл «eve.json» необходимо ввести следующую команду:

```
set suricata outputs eve-log enabled yes
```

где «eve-log» – идентификатор типа файла.

Возможно включение записи данных в файлы при использовании следующих идентификаторов:

- **«alert-debug»** – для записи предупреждений в файл «alert-debug.log»;
- **«eve-log»** – для записи уведомлений срабатываемых событий в файл «eve.json»;
- **«fast»** – для записи уведомлений срабатываемых правил в файл «fast.log»;
- **«http-log»** – для записи данных об http сессиях в файл «http.log»;
- **«pcap-log»** – для записи всех пакетов в файл «_log.pcap»;
- **«stats»** – для записи статистики в файл «stats.log»;
- **«tls-log»** – для записи данных о tls сессиях в файл «tls.log»;
- **«tls-store»** – для записи сертификатов tls сессий.

Для включения записи событий и предупреждений syslog необходимо ввести следующую команду:

```
set suricata outputs syslog enabled yes
```

Для включения журналирования в файл «suricata.log» необходимо ввести следующую команду:

```
set suricata logging outputs file enabled yes
```

Для включения журналирования в syslog необходимо ввести следующую команду:

```
set suricata logging outputs syslog enabled yes
```

Для включения обнаружения пакетов, переданных по определённому протоколу, необходимо ввести следующую команду:

```
set suricata app-layer protocols bittorrent-dht enabled yes
```

где «bittorrent-dht» – протокол.

Возможно включение обнаружения пакетов, переданных по следующим протоколам:

- **«bittorrent-dht»**;
- **«dcerpc»**;
- **«dhcp»**;
- **«dnp3»**;
- **«enip»**;
- **«ftp»**;
- **«ike»**;
- **«imap»**;
- **«http»**;
- **«http2»**;
- **«krb5»**;
- **«mqtt»**;
- **«modbus»**;
- **«nfs»**;
- **«ntp»**;
- **«pgsql»**;
- **«quic»**;
- **«rdp»**
- **«rfb»**;

- **«sip»**;
- **«smb»**;
- **«smtp»**;
- **«snmp»**;
- **«ssh»**;
- **«telnet»**;
- **«tftp»**;
- **«tls»**;
- **«dns tcp»** – dns over tcp;
- **«dns udp»** – dns over udp.

Для указания портов назначения, используемых при обнаружении пакетов по протоколу tls, необходимо ввести следующую команду:

```
set suricata app-layer protocols tls detection-ports dst-port 443
```

где «443» – порт. Приведён в качестве примера.

Возможно указание порта назначения при обнаружении пакетов по следующим протоколам:

- **«dnp3»**;
- **«enip»**;
- **«modbus»**;
- **«rfb»**;
- **«tls»**;
- **«smb»**;
- **«dns tcp»** – dns over tcp;
- **«dns udp»** – dns over udp.

Для настройки режима захвата для определённого интерфейса необходимо ввести следующую команду:

```
set suricata netmap interface eth0 copy-mode ips
```

где «eth0» – имя интерфейса; «ips» – режим предотвращения вторжений. Приведено в качестве примера.

Для настройки режима захвата для всех интерфейсов, для которых режим захвата не задан локально, необходимо ввести следующую команду:

```
set suricata netmap parameters copy-mode tap(ids)
```

где «tap(ids)» – режим обнаружения вторжений. Приведено в качестве примера.

Для настройки проверки контрольной суммы tcp пакетов необходимо ввести следующую команду:

```
set suricata netmap parameters checksum-checks yes
```

7.2 Обновление правил Suricata

Конфигурация источника правил:

Для настройки обновления правил с удалённого сервера необходимо ввести следующие команды:

```
set suricata update-rules remote-server ARMA authentication http-basic login admin1
set suricata update-rules remote-server ARMA authentication http-basic password examplePassw
set suricata update-rules remote-server ARMA url example.net
```

где «admin1» – логин; «examplePassw» – пароль; «example.net» – URL ресурса. Приведены в качестве примера.

Для настройки обновления правил с локального хранилища необходимо ввести следующую команду:

```
set suricata update-rules local-storage LOCAL path /path/to/storage
```

где «/path/to/storage» – путь к локальному хранилищу.

После настройки источника правил необходимо запустить обновления.

Для импорта правила с конкретного удалённого сервера необходимо ввести следующую команду:

```
admin@ngfwos:~$ run suricata update-rules remote-server ARMA
```

Для импорта правила со всех настроенных удалённых серверов необходимо ввести следующую команду:

```
admin@ngfwos:~$ run suricata update-rules remote-server all
```

Для импорта правила с конкретного локального хранилища необходимо ввести следующую команду:

```
admin@ngfwos:~$ run suricata update-rules local-storage LOCAL
```

Для импорта правила из всех настроенных локальных хранилищ необходимо ввести следующую команду:

```
admin@ngfwos:~$ run suricata update-rules local-storage all
```

Для сохранения всех правил в определённую директорию необходимо ввести следующую команду:

```
set suricata default-rule-path /path/to/rules
```

где «/path/to/rules» – путь.

7.3 Пример настройки правила

Для настройки СОВ необходимо выполнить следующие действия:

1. Ввести команды:

```
set suricata stream midstream-policy ignore
set suricata netmap interface eth0
set suricata netmap parameters copy-mode ips
set suricata netmap parameters threads auto
set suricata netmap parameters checksum-checks no
```

где «eth0» – имя интерфейса, приведено в качестве примера.

2. Зафиксировать изменения с помощью ввода команды **«commit»**.
3. В файл «suricata.rules», расположенному по пути «/var/lib/suricata/rules/suricata.rules», добавить следующее правило:
   - «drop icmp any any <> any any (msg:»icmp»; classtype:protocol-command-decode; sid:429496705; rev:1;)».
4. Ввести команду:

```
set suricata enable yes
```

5. Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

8 SYSLOG

Syslog – это стандарт отправки и регистрации сообщений о происходящих в системе событиях, используемый для удобства администрирования и обеспечения ИБ.

8.1 Настройка экспорта событий syslog

Для создания файла, содержащего сообщения системного журнала, необходимо ввести команду:

```
set system syslog file logfile facility all level alert
```

где «logfile» – имя файла, «all» – категория журналирования, «alert» – уровень журналирования.

Файл будет расположен по следующему пути «/var/log/user/».

Возможно журналирование по следующим категориям:

- **«all»** – все;
- **«kern»** – сообщения ядра;
- **«user»** – сообщения на уровне пользователя;
- **«mail»** – почта;
- **«daemon»** – системные демоны;
- **«auth»** – сообщения проверки подлинности;
- **«syslog»** – сообщения syslogd;
- **«lpr»** – подсистема линейного принтера;
- **«news»** – подсистема сетевых новостей;
- **«uucp»** – подсистема UUCP;
- **«cron»** – сообщения CRON;
- **«security»** – сообщения безопасности;
- **«ftp»** – сообщения FTP;
- **«ntp»** – сообщения NTP;
- **«logaudit»** – проверка журналов;
- **«logalert»** – предупреждения журналов;
- **«clock»** – сообщения демона clock;
- **«local0»** – локальное использование 0;
- **«local1»** – локальное использование 1;

- **«local2»** – локальное использование 2;
- **«local3»** – локальное использование 3;
- **«local4»** – локальное использование 4;
- **«local5»** – локальное использование 5;
- **«local6»** – локальное использование 6;
- **«local7»** – локальное использование 7.

Возможно журналирование по следующим уровням:

- **«all»** – все;
- **«emerg»** – чрезвычайная ситуация;
- **«alert»** – тревога;
- **«crit»** – критическое состояние;
- **«err»** – ошибка;
- **«warning»** – предупреждение;
- **«notice»** – извещение;
- **«info»** – информация;
- **«debug»** – отладка.

Для указания максимального размера создаваемого файла необходимо ввести команду:

```
set system syslog file logfile archive size 4096
```

где «4096» – размер записываемого файла в килобайтах, приведён в качестве примера. По достижении указанного размера будет создан новый файл для фиксации сообщений.

Для настройки ротации сохраняемых файлов по их количеству необходимо ввести команду:

```
set system syslog file logfile archive file 8
```

где «8» – количество файлов, приведено в качестве примера.

Для экспорта событий на удалённый хост необходимо ввести команду:

```
set system syslog host 192.168.2.1 facility all protocol tcp
```

где «192.168.2.1» – IP-адрес хоста; «tcp» – транспортный протокол. По умолчанию экспорт событий осуществляется по протоколу «UDP» через порт «514».

Для вывода сообщений журнала в консольный локальный интерфейс необходимо ввести команду **«show log firewall»**:

```
admin@ngfwos:~$ show log firewall
```

где «firewall» – применяемый фильтр сообщений.

Возможно отображение журнала с применением следующих фильтров:

- **«all»**;
- **«authorization»**;
- **«cluster»**;
- **«conntrack-sync»**;
- **«dhcp»**;
- **«directory»**;
- **«dns»**;
- **«file»**;
- **«firewall»**;
- **«https»**;
- **«image lldp»**;
- **«nat»**;
- **«openvpn»**;
- **«snmp»**;
- **«tail»**;
- **«vpn»**;
- **«vrrp»**.

9 DHCP-СЕРВЕР

DHCP-сервер используется для автоматического предоставления клиентам IP-адреса и других параметров, необходимых для работы в сети TCP/IP.

Для создания DHCP-сервера на **ARMA Стена** необходимо указать подсети и задать диапазон выдаваемых IP-адресов с помощью ввода следующих команд:

```
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24 range 0 start 192.168.70.10
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24 range 0 stop 192.168.70.100
```

где «192.168.70.0/24» – адрес сети; «192.168.70.10» – начальное значение диапазона IP-адресов; «192.168.70.100» – конечное значение диапазона IP-адресов. Приведены в качестве примера.

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

На ПК **«Client»** получить IP-адрес по протоколу DHCP.

10 УЧЕТНЫЕ ЗАПИСИ

10.1 Локальное добавление пользователя

Для создания пользовательской УЗ необходимо в режиме конфигурирования ввести следующие команды с указанием учётных данных:

```
set system login user User1 full-name "Fedor Volov"
```

где «User1» – логин, «Fedor Volov» – имя пользователя.

```
set system login user User1 authentication plaintext-password examplePassword
```

где «examplePassword» – пароль.

Учётные данные приведены в качестве примера.

10.2 Аутентификация

10.2.1 Radius

Radius – сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта пользователей, подключающихся к различным сетевым службам.

ARMA Стена поддерживает использование внешнего Radius-сервера для аутентификации пользователей.

Для добавления адреса radius-сервера необходимо ввести команду:

```
set system login radius server 192.168.2.34 key secretRadius
```

где «192.168.2.34» – IP-адрес radius-сервера, «secretRadius» – ключ radius-сервера.

По умолчанию используется порт «1812».

Для назначения порта radius-сервера следует ввести команду:

```
set system login radius server 192.168.2.34 port 21813
```

где «21813» – порт, приведён в качестве примера.

В случае необходимости отключения запроса Radius-сервера следует ввести команду:

```
set system login radius server 192.168.2.34 disable
```

Для проверки следует пройти аутентификацию в **ARMA Стена**, используя данные УЗ, заданной на radius-сервере.

11 ПРОКСИ

Прокси-сервер обеспечивает контролируемый доступ хостов локальной сети в сеть Интернет, а также защиту локальной сети от внешнего доступа.

11.1 Основные настройки прокси-сервера

Используемые в командах значения приведены в качестве примера.

1. Для указания доменного имени необходимо ввести следующую команду:

   ```
   set service webproxy append-domain example.net
   ```

   где «example.net» – доменное имя.

   Например, полученное значение «www/foo.html» будет преобразовано добавлением доменного имени «example.net» следующим образом – «www.example.net/foo.html».

2. Для указания размера кэша необходимо ввести следующую команду:

   ```
   set service webproxy cache-size 512
   ```

   где «512» – размер кэша, указываемый в мегабайтах.

   По умолчанию используется значение «100».

3. Для указания порта по умолчанию, на котором прокси-сервер будет прослушивать запросы, необходимо ввести следующую команду:

   ```
   set service webproxy default-port 8080
   ```

   где «8080» – номер порта.

   По умолчанию используется порт «3128».

4. Для блокирования прокси-сервером доступа к какому-либо домену необходимо ввести следующую команду:

   ```
   set service webproxy domain-block example.com
   ```

   где «example.com» – имя домена.

   Возможно указание домена первого уровня, например, «.org» для блокирования доступа к доменным именам, заканчивающимся на «.org».

5. Для отключения кэширования необходимо ввести следующую команду:

   ```
   set service webproxy domain-noncache example.net
   ```

   где «example.net» – имя домена.

6. Для указания адреса прослушивания необходимо ввести следующую команду:

```
set service webproxy listen-address 192.168.3.11
```

   где «192.168.3.11» – IP-адрес.

7. Для отключения режима прозрачного веб-прокси по определённому адресу прослушивания необходимо ввести следующую команду:

```
set service webproxy listen-address 192.168.3.11 disable-transparent
```

При отключённом режиме прозрачного прокси-сервера на клиентах необходимо указывать настройки прокси-сервера.

8. Для указания порта для адреса прослушивания необходимо ввести следующую команду:

```
set service webproxy listen-address 192.168.3.11 port 8080
```

   где «8080» – номер порта.

   По умолчанию используется порт «3128».

9. Для блокирования различных типов передаваемых данных необходимо ввести следующую команду:

```
set service webproxy reply-block-mime application/json
```

   где «application» – тип данных; «json» – формат файла.

   Возможно блокирование следующих типов данных:

   - **«application»**:
     - atom+xml;
     - EDI-X12;
     - EDIFACT;
     - font-woff;
     - gzip;
     - javascript;
     - json;
     - msword;
     - octet-stream;
     - ogg;
     - pdf;

- postscript;
- soap+xml;
- vnd.google-earth.kml+xml;
- vnd.mozilla.xul+xml;
- vnd.ms-excel;
- vnd.ms-excel.sheet.macroEnabled.12;
- vnd.ms-powerpoint;
- vnd.oasis.opendocument.graphics;
- vnd.oasis.opendocument.presentation;
- vnd.oasis.opendocument.spreadsheet;
- vnd.oasis.opendocument.text;
- vnd.openxmlformats-officedocument.presentationml.presentation;
- vnd.openxmlformats-officedocument.spreadsheetml.sheet;
- vnd.openxmlformats-officedocument.wordprocessingml.document;
- vnd.rar;
- x-bittorrent;
- x-tex;
- x-yaml;
- xml;
- xml-dtd;
- xop-xml;
- xhtml+xml;
- zip;

- **«audio»**:
  - aac;
  - basic;
  - L24;
  - mp4;
  - mpeg;
  - ogg;

    - vnd.rn-realaudio;
    - vnd.wave;
    - vorbis;
    - webm;
    - x-ms-wax;
    - x-ms-wma;
- **«example»**;
- **«image»**:
    - gif;
    - jpeg;
    - pjpeg;
    - png;
    - svg+xml;
    - tiff;
    - vnd.microsoft.icon;
    - vnd.wap.wbmp;
    - webp;
- **«message»**:
    - http;
    - imdn+xml;
    - partial;
    - rfc822;
- **«model»**:
    - example;
    - iges;
    - meh;
    - vrml;
    - x3d+binary;
    - x3d+vrml;
    - x3d+xml;

- **«multipart»**:
  - alternative;
  - encrypted;
  - form-data;
  - mixed;
  - related;
  - signed;
- **«text»**:
  - cache-manifest;
  - cmd;
  - css;
  - csv;
  - html;
  - javascript;
  - markdown;
  - php;
  - plain;
  - xml;
- **«video»**:
  - 3gpp;
  - 3gpp2;
  - mp4;
  - mpeg;
  - ogg;
  - quicktime;
  - webm;
  - x-ms-wmv;
  - x-flv;
  - x-msvideo.

10. Для указания способа аутентификации прокси необходимо ввести следующую команду:

```
set service webproxy authentication method kerberos
```

где «kerberos» – способ аутентификации.

ARMA Стена поддерживает следующие способы аутентификации:

- **«Kerberos»**;
- **«NTLM»**.

11. Для указания максимального количества запускаемых процессов аутентификации необходимо ввести следующую команду:

```
set service webproxy authentication children 4
```

где «4» – количество процессов аутентификации.

По умолчанию используется значение «5».

12. Для указания временного интервала между запросами учётных данных пользователя необходимо ввести следующую команду:

```
set service webproxy authentication credentials-ttl 45
```

где «45» – интервал в минутах.

По умолчанию используется значение «60».

13. При необходимости отображения информативного сообщения в окне авторизации следует ввести следующую команду:

```
set service webproxy authentication realm "EXAMPLE.COM"
```

где «EXAMPLE.COM» – текст сообщения.

11.2 Пример настройки кэширующего прокси-сервера

В качестве примера настройки кэширующего прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки прокси-сервера).

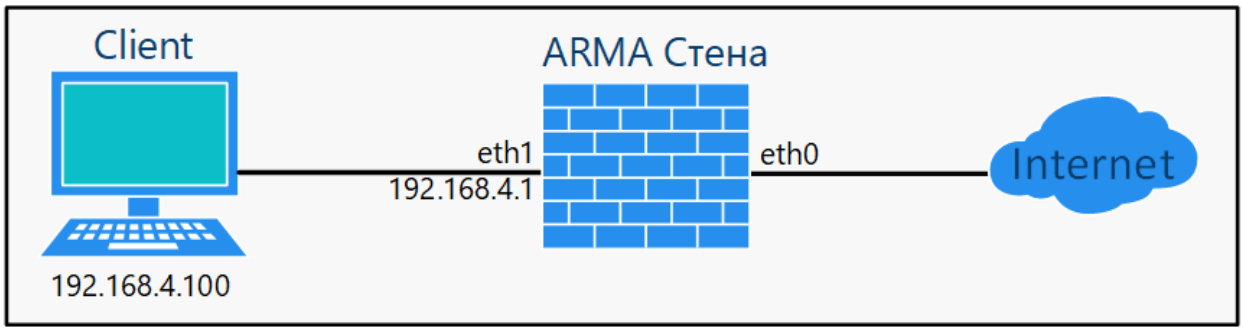

Рисунок – Схема стенда для настройки прокси-сервера

Предварительно **ARMA Стена** настроен следующим образом:

1. Для настройки переадресации DNS введены следующие команды:

```
set system name-server 8.8.8.8
set service dns forwarding cache-size 500
set service dns forwarding listen-address 192.168.4.1
set service dns forwarding allow-from 192.168.4.0/24
set service dns forwarding name-server 8.8.8.8
```

2. Для настройки правил NAT введены следующие команды:

```
set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 192.168.4.0/24
set nat source rule 10 translation address masquerade
```

   где «eth0» – интерфейс с доступом к сети интернет; «192.168.4.0/24» – адрес сети интерфейса «eth1», который будет подменяться IP-адресом интерфейса «eth0».

3. Для настройки МЭ введена следующая команда:

```
set firewall all-ping enable
```

4. Зафиксированы изменения с помощью ввода команд **«commit»** и **«save»**.

На ПК **«Client»** после перезапуска сетевого интерфейса обеспечен доступ к сети Интернет.

11.2.1 Настройка прокси-сервера

Для настройки прокси-сервера необходимо ввести следующие команды:

```
set service webproxy listen-address 192.168.4.1
set service webproxy listen-address 192.168.4.1 port 3128
set service webproxy listen-address 192.168.4.1 disable-transparent
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.2 Обновление черного списка

Для обновления черного списка необходимо ввести команды **«sudo -i»** и **«update webproxy blacklists»**:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~# update webproxy blacklists
```

После завершения обновления для выхода из режима суперпользователя и перезапуска службы прокси необходимо ввести команды **«'exit'»** и **«restart webproxy»**:

```
root@ngfwos:~# 'exit'
logout
admin@ngfwos:~$ restart webproxy
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.3 Настройка ПК «Client»

На ПК **«Client»** необходимо указать вручную следующие настройки прокси:

- **«HTTP прокси»** – «192.168.4.1»;
- **«порт»** – «3128»;
- **«HTTPS прокси»** – «192.168.4.1»;
- **«порт»** – «3128»;
- **«Не использовать прокси для»** – «localhost 127.0.0.0/8; ::1».

11.2.4 Настройка политик блокировки

В качестве примера приведён список команд для настройки политик блокировки различных ресурсов:

```
set service webproxy url-filtering squidguard source-group TEST address 192.168.220.0/24
set service webproxy url-filtering squidguard rule 20 source-group TEST
set service webproxy url-filtering squidguard rule 20 local-block youtube.com
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

В результате с ПК **«Client»** после перезапуска веб-браузера доступ к ресурсу «youtube.com» будет ограничен.

11.3 Технология единого входа

В качестве примера настройки SSO для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки SSO), со следующими параметрами:

- домен Active Directory – «example.com»;
- FQDN контроллера домена – «dc.example.com»;
- контроллер домена является DNS-сервером сети «LAN»;
- ПК **«Client»** введён в домен «example.com»;
- FQDN **ARMA Стена** – «ngfwos.example.com».

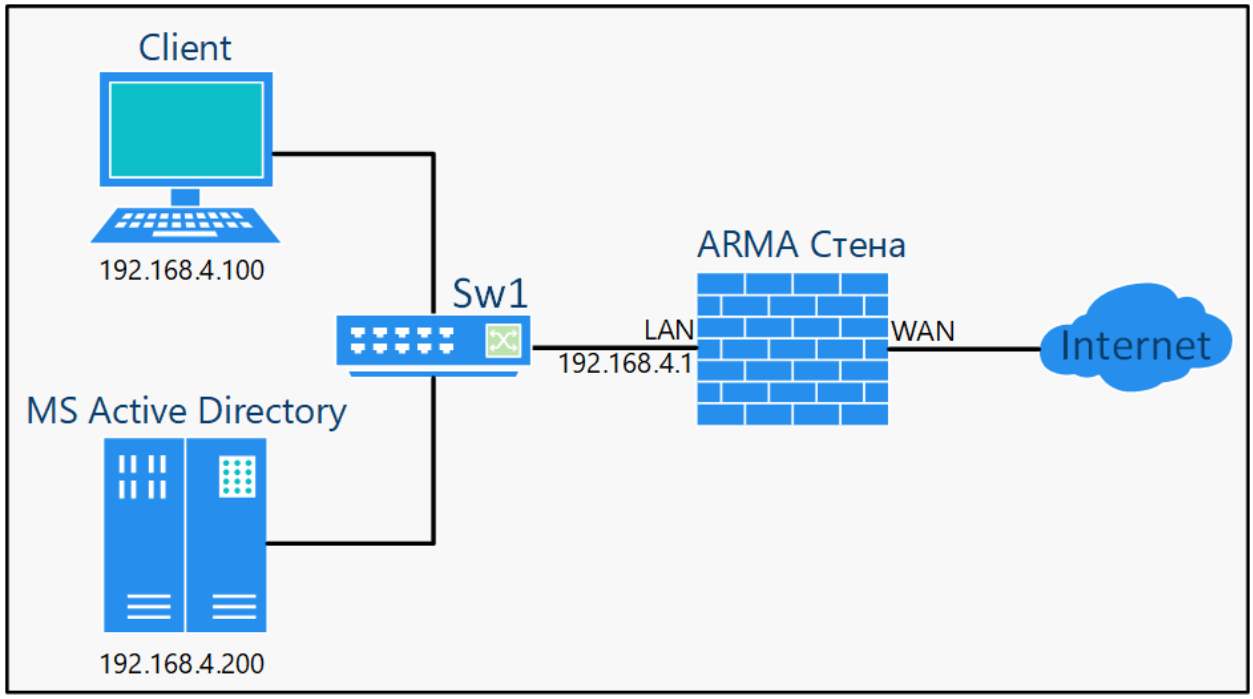

Рисунок – Схема стенда для настройки SSO

11.3.1 Аутентификация по протоколу Kerberos

В качестве примера настройки SSO по протоколу Kerberos для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки SSO).

Сервер AD предварительно настроен следующим образом:

- добавлены пользователи **«ngfwos»** и **«user1»**;
- создан домен **«example.com»**;
- сгенерирован файл «ngfwos.keytab» с помощью ввода в Powershell следующей команды:

```
ktpass -princ HTTP/ngfwos.example.com@EXAMPLE.COM -mapuser ngfwos@EXAMPLE.COM -pass Aa1234567 -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -out C:¥ngfwos.keytab
```

Полученный файл «ngfwos.keytab» перенесён на **ARMA Стена** и расположен по пути «/home/admin/ngfwos.keytab».

Для использования SSO на настроенном прокси-сервере необходимо выполнить следующие шаги:

1. Добавить DNS-записи на DNS-сервере.
2. Настроить **ARMA Стена** для работы с Active Directory.
3. Настроить прокси на ПК **«Client»**.

11.3.1.1 Добавление DNS-записей

На DNS-сервере необходимо создать записи:

- **Запись 1**:
  - **«Имя»** – «ngfwos»;
  - **«Полное доменное имя»** – «example.com.»;
  - **«IP-адрес»** – «192.168.4.1»;
- **Запись 2**:
  - **«Имя»** – «user1»;
  - **«Полное доменное имя»** – «example.com.»;
  - **«IP-адрес»** – «192.168.4.100»;
- **Запись 3**:
  - **«Имя»** – «dc»;
  - **«Полное доменное имя»** – «example.com.»;
  - **«IP-адрес»** – «192.168.4.200».

Записи создаются в соответствии с руководством пользователя используемого DNS-сервера.

На ПК **«Client»** необходимо войти в домен «example.com» под пользователем «user1». В качестве DNS-сервера указать «192.168.4.200».

11.3.1.2 Настройка ARMA Стена для работы с Active Directory

Для настройки **ARMA Стена** необходимо в режиме конфигурирования ввести следующие команды:

```
set service webproxy authentication kerberos domain example.com
```

где «example.com» – имя домена;

```
set service webproxy authentication kerberos domain-controller dc.example.com
```

где «dc.example.com» – FQDN контроллера домена;

```
set service webproxy authentication kerberos host ngfwos.example.com
```

где «ngfwos.example.com» – FQDN текущего хоста;

```
set service webproxy authentication kerberos kdc dc.example.com
```

где «dc.example.com» – FQDN сервера распространения ключей;

```
set service webproxy authentication kerberos keytab /home/admin/ngfwos.keytab
```

где «/home/admin/ngfwos.keytab» – путь к файлу «ngfwos.keytab»;

```
set service webproxy authentication kerberos realm EXAMPLE.COM
```

где «EXAMPLE.COM» – приветственное сообщение;

```
set service webproxy listen-address 192.168.4.1 port 2000
set service webproxy listen-address 192.168.4.1 disable-transparent
set service webproxy authentication enable
```

где «192.168.4.1» – IP-адрес **ARMA Стена**; «2000» – номер порта;

```
set system name-server 192.168.4.200
```

где «192.168.4.200» – IP-адрес сервера AD.

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.3.1.3 Настройка прокси на ПК «Client»

На ПК **«Client»** указать настройки прокси для следующих параметров:

- **«HTTP прокси»** – «ngfwos.example.com»;
- **«Порт»** – «2000».

11.3.1.4 Проверка

На ПК **«Client»** с помощью утилиты «Wireshark» выполнить захват трафика при подключении к какому-либо ресурсу сети Интернет.

В поле информации захваченного пакета «Proxy Authentication Required» будет присутствовать строка следующего вида: «Proxy-Authenticate: Negotiate¥r¥n».

11.3.2 Аутентификация пользователей по протоколу NTLMv2

В качестве примера настройки SSO по протоколу NTLMv2 для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки SSO).

Сервер AD предварительно настроен следующим образом:

- добавлены пользователи **«ngfwos»** и **«user1»**;
- создан домен **«example.com»**.

Для использования SSO на настроенном прокси-сервере необходимо выполнить следующие шаги:

1. Добавить DNS-записи на DNS-сервере.
2. Настроить **ARMA Стена** для работы с Active Directory.

3. Настроить прокси на ПК **«Client»**.

11.3.2.1 Добавление DNS-записей

На DNS-сервере необходимо создать записи:

- **Запись 1**:
  - **«Имя»** – «ngfwos»;
  - **«Полное доменное имя»** – «example.com.»;
  - **«IP-адрес»** – «192.168.4.1»;
- **Запись 2**:
  - **«Имя»** – «user1»;
  - **«Полное доменное имя»** – «example.com.»;
  - **«IP-адрес»** – «192.168.4.100»;
- **Запись 3**:
  - **«Имя»** – «dc»;
  - **«Полное доменное имя»** – «example.com.»;
  - **«IP-адрес»** – «192.168.4.200».

Записи создаются в соответствии с руководством пользователя используемого DNS-сервера.

На ПК **«Client»** необходимо войти в домен «example.com» под пользователем «user1». В качестве DNS-сервера указать «192.168.4.200».

11.3.2.2 Настройка ARMA Стена для работы с Active Directory

Для настройки **ARMA Стена** необходимо в режиме конфигурирования ввести следующие команды:

```
set service webproxy authentication ntlm netbios-name NGFWOS
```

где «NGFWOS» – NetBIOS-имя устройства в верхнем регистре;

```
set service webproxy authentication ntlm password Aa1234567
```

где «Aa1234567» – пароль пользователя **ARMA Стена** в AD, приведён в качестве примера;

```
set service webproxy authentication ntlm username user1
```

где «user1» – логин пользователя **ARMA Стена** в AD;

```
set service webproxy authentication ntlm realm EXAMPLE.COM
```

где «EXAMPLE.COM» – приветственное сообщение;

```
set service webproxy authentication ntlm workgroup EXAMPLE
```

где «EXAMPLE» – NetBIOS-имя домена AD, в верхнем регистре;

```
set service webproxy listen-address 192.168.4.1 port 2000
set service webproxy listen-address 192.168.4.1 disable-transparent
set service webproxy authentication enable
```

где «192.168.4.1» – IP-адрес **ARMA Стена**; «2000» – номер порта;

```
set system name-server 192.168.4.200
```

где «192.168.4.200» – IP-адрес сервера AD.

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.3.2.3 Настройка прокси на ПК «Client»

На ПК **«Client»** указать настройки прокси для следующих параметров:

- **«HTTP прокси»** – «ngfwos.example.com»;
- **«Порт»** – «2000».

11.3.2.4 Проверка

На ПК **«Client»** с помощью утилиты «Wireshark» выполнить захват трафика при подключении к какому-либо ресурсу сети Интернет.

В поле информации захваченного пакета «Proxy Authentication Required» будет присутствовать строка следующего вида: «Proxy-Authenticate: Negotiate¥r¥n».

11.4 Группы пользователей

Для управления группами необходимо наличие конфигурации SSO по протоколу «Kerberos» или «NTLM».

Для запрета доступа пользователям какой-либо группы AD необходимо ввести следующую команду:

```
set service webproxy user-group users1gr access deny
```

где «users1gr» – имя группы пользователей. Приведено в качестве примера.

Для блокирования доступа пользователей группы к определённым доменам необходимо ввести следующие команды:

```
set service webproxy user-group users1gr access permit
set service webproxy user-group users1gr block-domain .youtube.com
```

где «.youtube.com» – доменное имя.

12 VPN

VPN – это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например сети Интернет.

12.1 OpenConnect

OpenConnect – ПО с открытым исходным кодом, используемое для реализации VPN.

12.1.1 Подключение через VPN-клиент

Для предварительной настройки NAT и МЭ на **ARMA Стена** введены следующие команды:

```
set nat source outbound-interface interface eth0
set nat source address 192.168.4.0/24
set nat source translation masquerade
set firewall all-ping enable
```

Зафиксированы изменения с помощью команд **«commit»** и **«save»**.

На ПК **«Client»** установлено соответствующее ПО OpenConnect.

Для настройки подключения через VPN-клиент OpenConnect необходимо выполнить следующие шаги:

1. Сгенерировать ключ и сертификаты.
2. Настроить OpenConnect.

12.1.1.1 Генерация ключа и сертификатов

Для генерации ключа и сертификатов сервера и центра сертификации необходимо ввести следующие команды:

```
admin@ngfwos:~$ generate wireguard default-keypair
admin@ngfwos:~$ sudo su
root@ngfwos:/home/admin# chmod 777 /config/auth
root@ngfwos:/home/admin# 'exit'
```

При вводе двух последующих команд:

```
admin@ngfwos:~$ openssl req -newkey rsa:4096 -new -nodes -x509 -days 3650 -keyout /config/auth/server.key -out /config/auth/server.crt
admin@ngfwos:~$ openssl req -new -x509 -key /config/auth/server.key -out /config/auth/ca.crt
```

необходимо указать следующие значения параметров сертификатов:

- ввести **«RU»** на запрос:

```
Country Name (2 letter code) [AU]:
```

- ввести **«MO»** на запрос:

```
State or Province Name (full name) [Some-State]:
```

- ввести **«Moscow»** на запрос:

```
Locality Name (eg, city) []:
```

- ввести **«IWARMA»** на запрос:

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
```

- ввести **«IT»** на запрос:

```
Organization Unit Name (eg, section) []:
```

- ввести **«example.ru»** на запрос:

```
Common Name (eg, server FQDN or YOUR name) []:
```

- ввести **«mail@example.ru»** на запрос:

```
Email Address []:
```

Значения параметров сертификатов приведены в качестве примера.

12.1.1.2 Настройка OpenConnect

Для настройки OpenConnect необходимо ввести следующие команды:

```
set vpn openconnect authentication local-users username user1 password examplepssw
```

где «user1» – логин; «examplepssw» – пароль.

```
set vpn openconnect authentication mode local
```

где «local» – режим аутентификации.

```
set vpn openconnect network-settings client-ip-settings subnet 100.64.0.0/24
set vpn openconnect network-settings name-server 10.1.1.1
set vpn openconnect network-settings name-server 10.1.1.2
set vpn openconnect ssl ca-cert-file /config/auth/ca.crt
set vpn openconnect ssl cert-file /config/auth/server.crt
set vpn openconnect ssl key-file /config/auth/server.key
```

где «/config/auth/ca.crt» – путь к сертификату центра сертификации; «/config/auth/server.crt» – путь к сертификату сервера; «/config/auth/server.key» – путь к ключу.

12.1.1.3 Подключение клиента

Для подключения на ПК **«Client»** выполнить следующие действия:

- перейти в раздел настройки сетевых параметров;
- выбрать «MultiProtocol VPN OpenConnect» для нового подключения;
- указать IP-адрес интерфейса с доступом к сети Интернет «203.0.113.87» в поле параметра **«Шлюз»**;
- сохранить, включить и пройти аутентификацию в появившемся окне, введя учётные данные «user1» и «examplepssw».

где «203.0.113.87» – IP-адрес приведён в качестве примера.

В случае появления при первом подключении предупреждающего окна нажать **кнопку «Connect anyway»**.