

BI.ZONE Secure SD-WAN

Обзор страницы настройки VNF Firewall

Введение

Страница **VNF Firewall** предназначена для настройки VNF Firewall на CPE. Для того чтобы пройти на данную страницу, осуществите переход по пути: **Security Orchestrator → VNFs → CPE-Имя_CPE/firewall**.

Страница настройки VNF Firewall состоит из следующих вкладок:

1. Rules.
2. Zones.
3. B/W Lists.
4. Commit history.
5. System.




Вкладка Rules

Информация

Процесс добавления и настройки VNF на CPE описан в подразделе [Настройка функции VNF Firewall на CPE](#).

Вкладка **Rules** предназначена для мониторинга и настройки правил и шаблона правил VNF Firewall.

На странице вкладки указаны такие параметры, как:


1. **Name** — имя правила или шаблона правил.
2. **Action** — действие, которое необходимо выполнить правилу в случае, если пакет будет соответствовать заданным критериям.
3. **From** — одна или несколько зон адреса сетевого интерфейса CPE, отправивший пакет.
4. **To** — одна или несколько зон адреса сетевого интерфейса CPE, получивший пакет.
5. **Source** — один или несколько адресов отправителя. Для просмотра отчета по параметру **Source** (имя и IP-адрес) нажмите на имя адреса.
6. **Destination** — один или несколько адресов получателя. Для просмотра отчета по параметру **Destination** (имя и IP-адрес) нажмите на имя адреса.
7. **Service** — один или несколько сервисов, которые будут выполняться получателем. Для просмотра отчета по параметру **Service** (имя и используемый порт) нажмите на сервис.
8. **NAT** — показывает состояние настройки NAT. Настройка NAT описана в подразделе [Настройка NAT](#).
9. **Log** — счетчик срабатывания правил. Данный счетчик начнет функционировать в том случае, если при настройке функции VNF Firewall был включен флажок **Log**. Срабатывает счетчик когда выполняются условия правила:
 - а. Значение счетчика зависит от выбранного действия в раскрывающемся списке **Action**:
 - i. Если выбрано **Accept** или **NAT**, значение счетчика указывает на количество сессий, которые попали под условия данного правила.
 - ii. Если выбрано **Drop** или **Reject**, значение счетчика указывает на количество пакетов, которые попали под условия данного правила.
 - б. Для просмотра графика логa нажмите на кнопку .


с. Для обнуления счетчика лог нажмите на кнопку .

← CPE - CyberEdge-300_CPE_0 / firewall ONLINE Synchronized Apply


Rules Zones B/W Lists Commit history System

Name	Action	From	To	Source	Destination	Service	NAT	Log
ZMMay		LAN	OVERLAY	AD-ANY	AD-WebJuc	ANY	Source → Destination	
UppVdr		LAN	WAN	AD-ANY	AD-ANY	ANY	empty	
Default Template								
test1		WAN	LAN WAN	n/a	AD-ANY	COMP	empty	
Default action		Any	Any	Any	Any	ANY		Disabled

Для редактирования правила или шаблона правил нажмите на кнопку .

При нажатии на кнопку  в строке с шаблоном правил, появятся следующие опции:

- Опция **Reorder**. Предназначена для переупорядочивания шаблона правил. При нажатии на эту опцию, откроется диалоговое окно **Reordering rule**, в котором:
 - поле **Head** — шаблон правил переместится в начало списка и будет выполняться самым первым;
 - поле **Tale** — шаблон правил переместится в конец списка и будет выполняться последним;
 - поле **Before rule** — в случае выбора этой позиции всплывет поле **Before rule**. В нем выберите то правило, до которого будет выполняться шаблон правил, к которому применяется порядок **Before rule**;
 - поле **After rule** — в случае выбора этой позиции всплывет поле **After rule**. В нем выберите то правило, после которого будет выполняться шаблон правил, к которому применяется порядок **After rule**.
- Опция **Swap to another template**. Предназначена для переопределения шаблона правил. Процесс создания шаблона правил описан в подразделе [Создание шаблона правил](#).
- Опция **Delete**. Предназначена для удаления шаблона правил.

При нажатии на кнопку  в строке с правилом, появятся следующие опции:

- Опция **Reorder**. Предназначена для переупорядочивания правила. При нажатии на эту опцию, откроется диалоговое окно **Reordering rule**, в котором:
 - поле **Head** — правило переместится в начало списка и будет выполняться самым первым;
 - поле **Tale** — правило переместится в конец списка и будет выполняться последним;
 - поле **Before rule** — в случае выбора этой позиции всплывет поле **Before rule**. В нем выберите то правило, до которого будет выполняться правило, к которому применяется порядок **Before rule**;

- d. поле **After rule** — в случае выбора этой позиции всплывет поле **After rule**. В нем выберите то правило, после которого будет выполняться правило, к которому применяется порядок **After rule**;
 - e. поле **Before template** — правило переместится в шаблон правил, который располагается ниже в списке;
 - f. поле **After template** — правило переместится из шаблона правил выше по списку.
2. Опция **Clone**. Предназначена для клонирования правила.
 3. Опция **Delete**. Предназначена для удаления шаблона правил.



Вкладка Zones (на странице настройки VNF Firewall)

Информация

Процесс создания зоны описан в подразделе [Создание зон](#).

Процесс настройки зоны описан в подразделе [Настройки во вкладке Zones](#).

Вкладка **Rules** предназначена для настройки и управления зонами в которых будет функционировать выбранная VNF Firewall.

На странице вкладки указаны такие параметры, как:

1. **Name** — имя зоны.
2. **Interfaces** — сети, к которым привязана зона.
3. **Actions** — действия, которые возможно совершить с зоной.

← CPE - CyberEdge-300_CPE_0 / firewall ONLINE Synchronized

Rules **Zones** B/W Lists Commit history System

+ Bind zone		Unbind zones	
<input type="checkbox"/>	Name 1	Interfaces 2	Actions 3
<input type="checkbox"/>	OVERLAY	Pre-defined interface list	
<input type="checkbox"/>	WAN	Pre-defined interface list	
<input type="checkbox"/>	LAN	bMHPvU EWHFJN qgzDil JboKGv zYbEaO NiRBca	
<input type="checkbox"/>	RA_VPN	Pre-defined interface list	
<input type="checkbox"/>	bFEQeX	XiEIXI	
<input type="checkbox"/>	NuwBrc	PMHmXh	
<input type="checkbox"/>	plaFbz	DILYcB	

Для удаления зоны из VNF Firewall выполните следующие действия:

1. Выберите зону, нажав на флажок.
2. Нажмите на кнопку .

Вкладка B/W Lists

Информация

Процесс создания перечня описан в подразделе [Создание перечня с разрешенными и/или запрещенными IP-адресами](#).

Процесс привязки перечня описан в подразделе [Настройки во вкладке B/W Lists](#).

Вкладка **B/W Lists** предназначена для управления перечнями с разрешенными и/или запрещенными IP-адресами на VNF Firewall.

На странице вкладки указаны такие параметры, как:

1. **Name** — имя списка.
2. **Behavior** — тип поведения перечня: черный (black) или белый (white) список.
3. **Actions** — действия, которые возможно совершить с перечнем.

← CPE - CyberEdge-300_CPE_0 / firewall ONLINE Synchronized

Rules Zones **B/W Lists** Commit history ⌵ System

+ Bind BWLs Unbind BWLs

<input type="checkbox"/>	Name	Behavior	Actions
<input type="checkbox"/>	FsXSbz	Black	
<input type="checkbox"/>	NRhosh	Black	
<input type="checkbox"/>	ZJyGaD	White	
<input type="checkbox"/>	cKMCYd	Black	
<input type="checkbox"/>	pCLtgq	White	

Для удаления перечня из VNF Firewall выполните следующие действия:

1. Выберите перечень, нажав на флажок.
2. Нажмите на кнопку

Вкладка Commit history

Во вкладке **Commit history** ведется учет коммитов изменений на VNF Firewall.

На странице вкладки указаны такие параметры, как:

1. **Name** — имя коммита.
2. **Date** — дата создания коммита.
3. **Modified entities** — измененные объекты.
4. **Actions** — действия, которые возможно совершить с коммитом.

← CPE - CyberEdge-300_CPE_0 / firewall ONLINE Synchronized

Rules Zones B/W Lists **Commit history** System

Name	Date	Modified entities	Actions
Deleting rules [191, 198, 204, 211, 217, 224]	30.01.2024 14:21:42	rules, config	
Adding rule LAN to WAN (test_cancel_to_all_if_not_all_vnfs_modified)	30.01.2024 14:21:16	rules, config	
Add rule LAN to WAN (test_cancel_to_all_if_not_all_vnfs_modified)	30.01.2024 14:20:50	rules, config	
Adding rule LAN to WAN (test_confirm_to_all_if_not_all_vnfs_modified)	30.01.2024 14:20:35	rules, config	
Adding rule LAN to WAN (test_confirm_to_all_if_not_all_vnfs_modified)	30.01.2024 14:20:20	rules, config	
Adding rule LAN to WAN (test_apply_to_all_if_not_all_vnfs_modified)	30.01.2024 14:20:05	rules, config	
Adding rule LAN to WAN (test_apply_to_all_if_not_all_vnfs_modified)	30.01.2024 14:19:50	rules, config	
1234	30.01.2024 14:18:54	rules, config	
[autotag] Edit "iface"	30.01.2024 13:42:04	ifaces	
[autotag] Edit "iface"	30.01.2024 13:41:58	ifaces	

Доступные действия с коммитами:

1. — делает коммит активным для просмотра параметров VNF Firewall, но без применения их. При активации режима появляется надпись в верхнем правом углу **View mode**.

Доступные действия в данном режиме:

- а. Восстановление параметров выбранного коммита — кнопка **Restore**.
- б. Выхода из этого режима — кнопка **Exit**.

2. — восстанавливает настройки выбранного коммита.

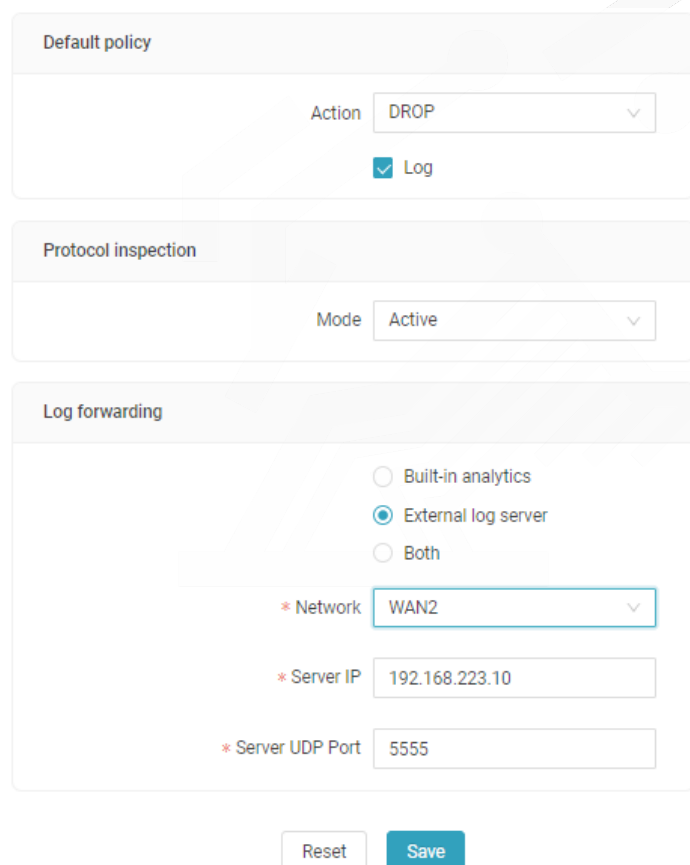
Вкладка System

Информация

Описание блоков данной вкладки приведен в подразделе [Настройки во вкладке System](#).

Вкладка **System** предназначена для установки работы VNF Firewall по умолчанию, включения/выключения функции Protocol inspection, а также за настройку отправки журналов событий и активности VNF Firewall на внешний сервер и встроенную аналитику.

Вкладка **System** состоит из следующих блоков: **Default policy**, **Protocol inspection**, **Log forwarding**.



The screenshot displays the 'System' configuration page for VNF Firewall. It features three main sections: 'Default policy', 'Protocol inspection', and 'Log forwarding'. The 'Default policy' section has an 'Action' dropdown set to 'DROP' and a checked 'Log' checkbox. The 'Protocol inspection' section has a 'Mode' dropdown set to 'Active'. The 'Log forwarding' section includes radio buttons for 'Built-in analytics', 'External log server' (which is selected), and 'Both'. Below these are three required fields: '* Network' (set to 'WAN2'), '* Server IP' (set to '192.168.223.10'), and '* Server UDP Port' (set to '5555'). At the bottom are 'Reset' and 'Save' buttons.

Default policy	
Action	DROP
Log	<input checked="" type="checkbox"/>

Protocol inspection	
Mode	Active

Log forwarding	
<input type="radio"/> Built-in analytics	
<input checked="" type="radio"/> External log server	
<input type="radio"/> Both	
* Network	WAN2
* Server IP	192.168.223.10
* Server UDP Port	5555

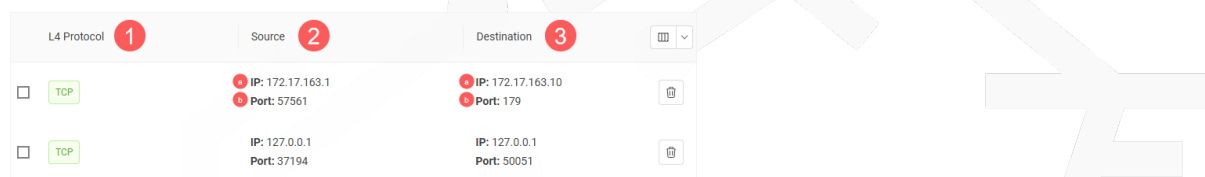
Reset Save

Вкладка Active sessions


Вкладка **Active Sessions** предназначена для мониторинга текущих сетевых сессий через VNF Firewall.

На странице вкладки указаны следующие параметры сессий по умолчанию, как:

1. **L4 Protocol** — протокол уровня 4 модели OSI, используемый в сессии (например, TCP или UDP).
2. **Source:**
 - a. **IP** — IP-адрес источника, отправляющий пакеты в текущей сессии.
 - b. **Port** — TCP/UDP-порт источника, с которого отправляются данные.
3. **Destination:**
 - a. **IP** — IP-адрес назначения, получающий пакеты в текущей сессии.
 - b. **Port** — TCP/UDP-порт назначения, на который отправляются данные.



L4 Protocol	Source	Destination
<input type="checkbox"/> TCP	IP: 172.17.163.1 Port: 57561	IP: 172.17.163.10 Port: 179
<input type="checkbox"/> TCP	IP: 127.0.0.1 Port: 37194	IP: 127.0.0.1 Port: 50051

Кнопка  позволяет отобразить или скрыть параметры сессий. Для скрытия или отображения параметра нажмите на переключатель рядом с параметром. Для возврата отображения параметров по умолчанию нажмите на кнопку [Reset to default view](#).

Дополнительные параметры, которые возможно отобразить:

1. **Reverse source IP** — IP-адрес источника пакета в обратном направлении. Используется для отображения информации о возвратных пакетах в сессии.
2. **Reverse source port** — TCP/UDP-порт источника в обратном направлении. Используется для отображения информации о возвратных пакетах в сессии.
3. **Reverse destination IP** — IP-адрес назначения пакета в обратном направлении. Используется для отображения информации о возвратных пакетах в сессии.
4. **Reverse destination port** — TCP/UDP-порт назначения в обратном направлении. Используется для отображения информации о возвратных пакетах в сессии.
5. **ICMP type** — тип ICMP-сообщения (например, Echo Request или Echo Reply).
6. **ICMP code** — код ICMP-сообщения, который уточняет информацию о типе ICMP (например, при ошибке маршрутизации).

☰

▼

Reset to default view

	L4 Protocol	<input checked="" type="checkbox"/>
	Source IP	<input checked="" type="checkbox"/>
	Source port	<input checked="" type="checkbox"/>
	Destination IP	<input checked="" type="checkbox"/>
	Destination port	<input checked="" type="checkbox"/>
1	Reverse source IP	<input type="checkbox"/>
2	Reverse source port	<input type="checkbox"/>
3	Reverse destination IP	<input type="checkbox"/>
4	Reverse destination port	<input type="checkbox"/>
5	ICMP type	<input type="checkbox"/>
6	ICMP code	<input type="checkbox"/>

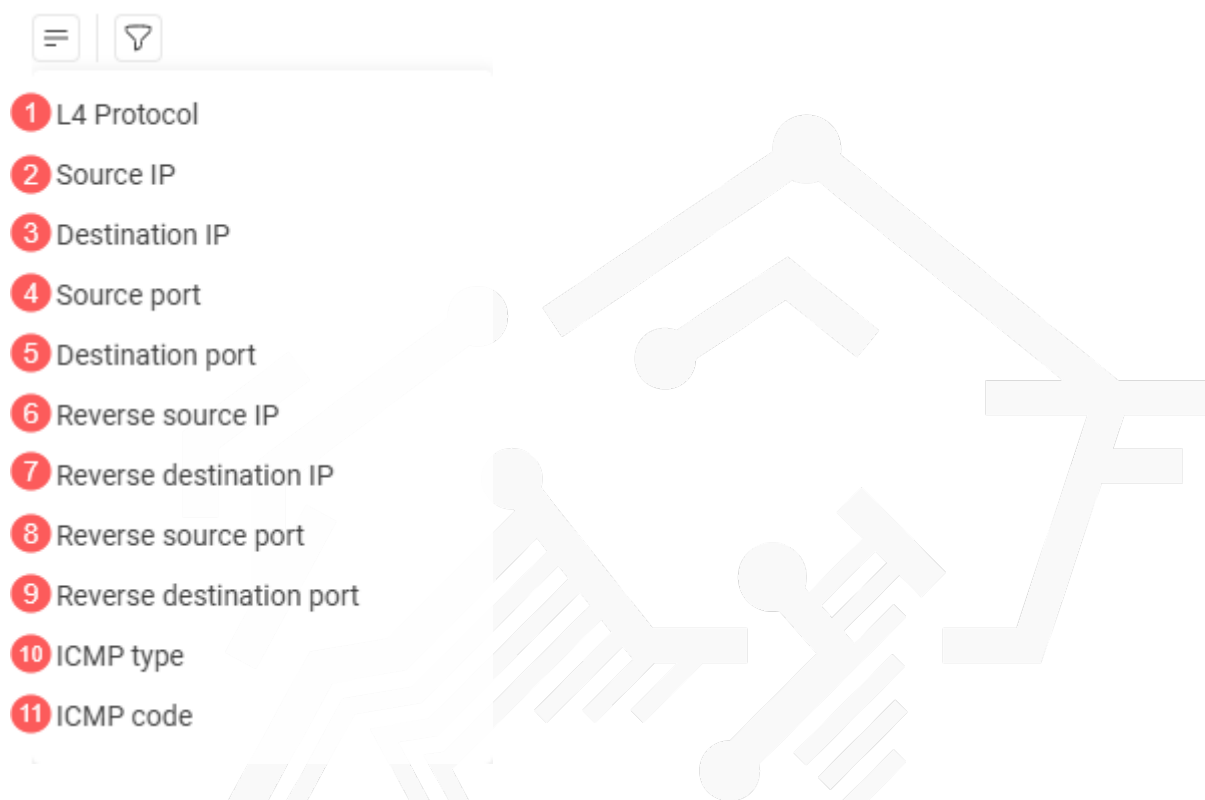
Для обновления списка сессий в ручном режиме нажмите на кнопку **Update** . Для установки автоматического обновления списка сессий нажмите на раскрывающийся список у кнопки **Update** и выберите интервал обновления.

Кнопка **≡** предназначена для сортировки сессий.


Кнопка **🔍** предназначена для настройки фильтрации сессий по различным параметрам:

1. **L4 Protocol** — фильтрация по протоколу уровня 4 модели OSI. В дополнительном поле параметра **L4 Protocol** имеются следующие варианты ввода:
 - а. Ввод названия или номера протокола.
 - б. Выбор одного или нескольких протоколов из списка.
2. **Source IP** — фильтрация по IP-адресу источника, отправляющего пакеты.
3. **Destination IP** — фильтрация по IP-адресу назначения, получающего пакеты.
4. **Source port** — фильтрация по исходному порту, через который передаются пакеты.
5. **Destination port** — фильтрация по порту назначения.
6. **Reverse source IP** — фильтрация по IP-адресу обратного источника (IP-адрес с которого возвращаются данные).

7. **Reverse destination IP** — фильтрация по IP-адресу обратного назначения (сессии, где пакеты возвращаются на конкретный IP-адрес).
8. **Reverse source port** — фильтрация по порту обратного источника (сессии, где порт для возвратных данных отличается от исходного).
9. **Reverse destination port** — фильтрация по порту обратного назначения, который используется для возврата данных.
10. **ICMP type** — фильтрация по типу ICMP-сообщений.
11. **ICMP code** — фильтрация по коду ICMP.



Для завершения сессии выполните следующие действия:

1. Выберите одну или несколько сессий, нажав на флажок рядом с сессией и нажмите на кнопку `Delete session`.
2. Либо нажмите на кнопку  напротив сессии.