Arbor Networks

Продуктовая линейка SP/TMS

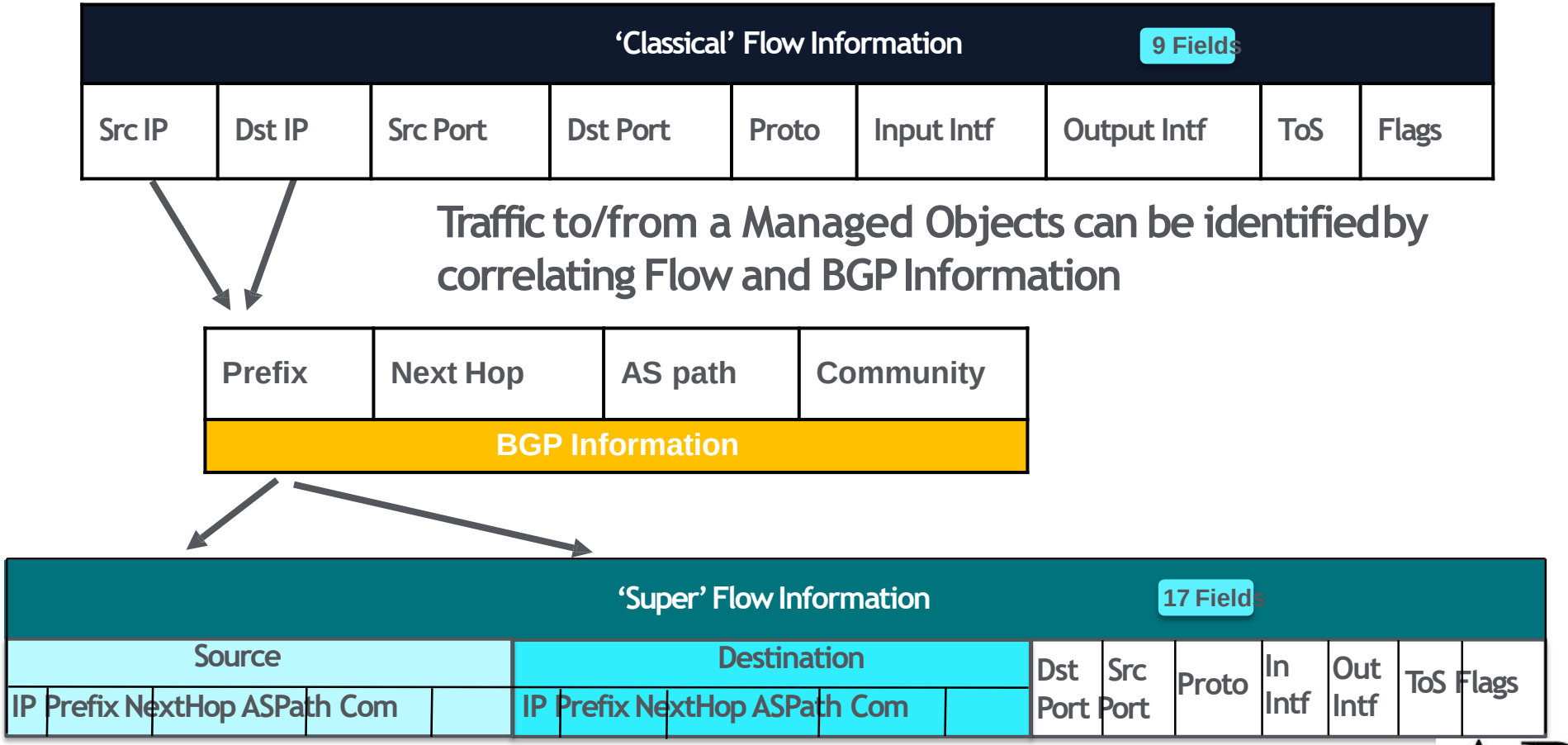
Визуализация – Знай свою сеть

- Какой трафик в моей сети?
- Как он меняется со временем?
- Где узкие места в моей сети?
- Где нужно нарастить емкость каналов?
- Какова загрузка моих ресурсов?
- Как мне спланировать маршрутизацию?
- К какому оператору лучше подключиться?
- Как растет IPv6 трафик в моей сети?
- Есть ли у меня IPv6 туннели?

ARBOR™ NETWORKS

Насыщение FLOW

SP does a longest match on source IP and destination IP of the flow to the prefixes in BGP routes



ARBOR NETWORKS

Визуализация = Arbor SP

- 350+ преднастроенных отчетов
  - Возможность создавать «свои» отчеты
- WEB Портал
  - 700 одновременных пользователей (20k в БД)
  - Разграничение прав доступа (Radius/Tacacs)
- Отчеты для начальства (Executive reports)
  - Вся сеть в одном отчете.
- Atlas Global DDoS Report
  - Глобальное состояние мира DDoS за последний месяц
  - Создается ASERT
  - Данные из ATLAS

Автоматизация ключ к успеху

- Подход “Fast Flood”
  - Время появления сигнала о DDoS атаки от 1 секунды (10 - 15 секунд в среднем)
- Авто – Митигация
  - Автоматическое перенаправление трафика на систему очистки при атаке
  - Молниеносное подавление атаки
- Автоматический Offload FlowSpec фильтров на маршрутизаторы
  - Маршрутизаторы «становятся» системами очистки с огромной емкостью
- Rest API
  - Цель: достигнуть паритета между функционалом WEB UI и REST API
  - Дополнительная гибкость, высокий уровень кастомизации, дополнительный функционал и отчеты, возможность интеграции с различными внешними системами

ARBOR™ NETWORKS

Архитектура SP/TMS

Коллекторы Телеметрии

- Визуализация трафика, проходящего через Peering/Transit/Backbone, выявление аномалий и угроз
- Возможность мониторинга трафика клиентов на границе сети (Edge)

Система очистки трафика

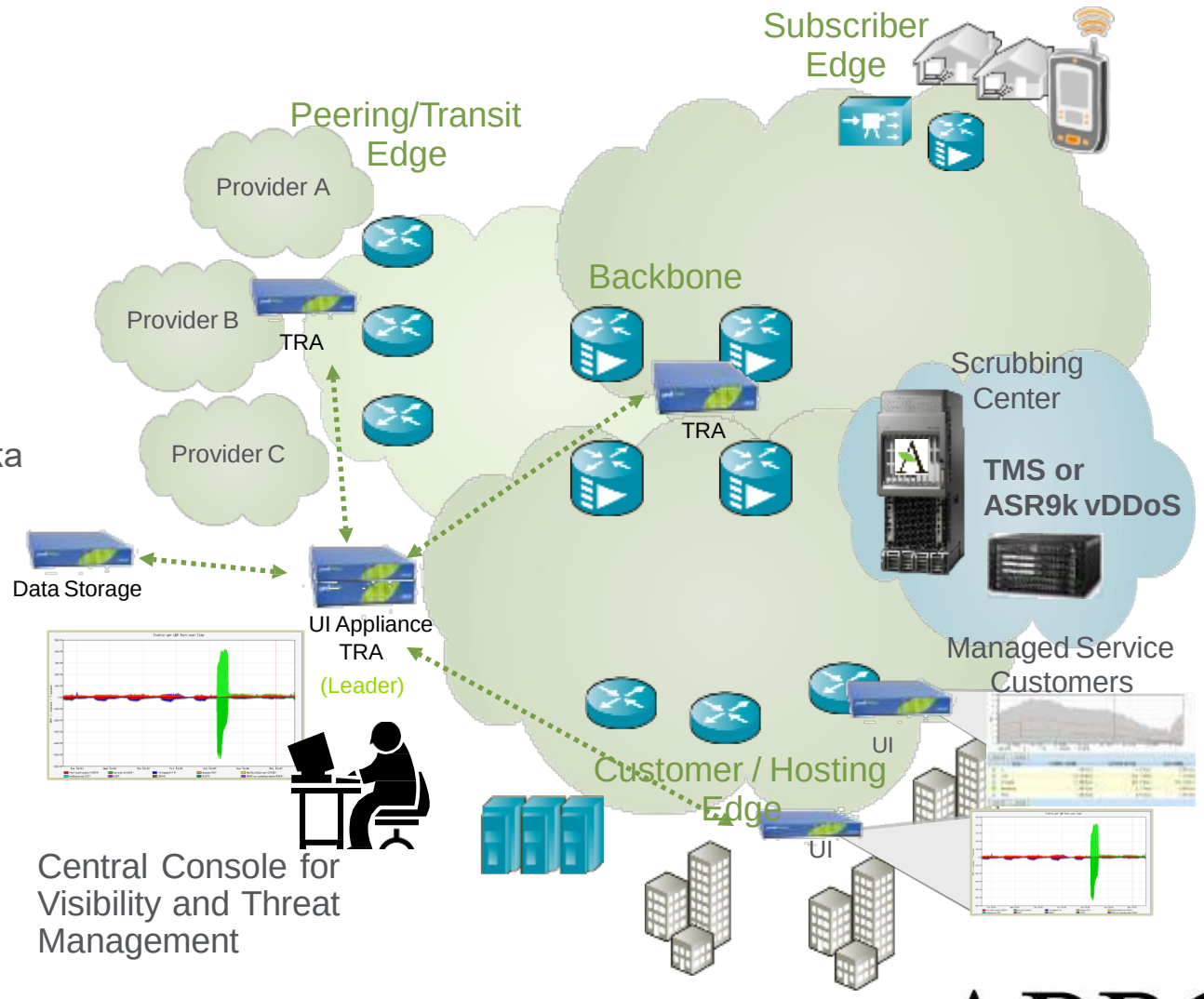
“Хирургическое” выделение зловредного трафика

Объекты мониторинга

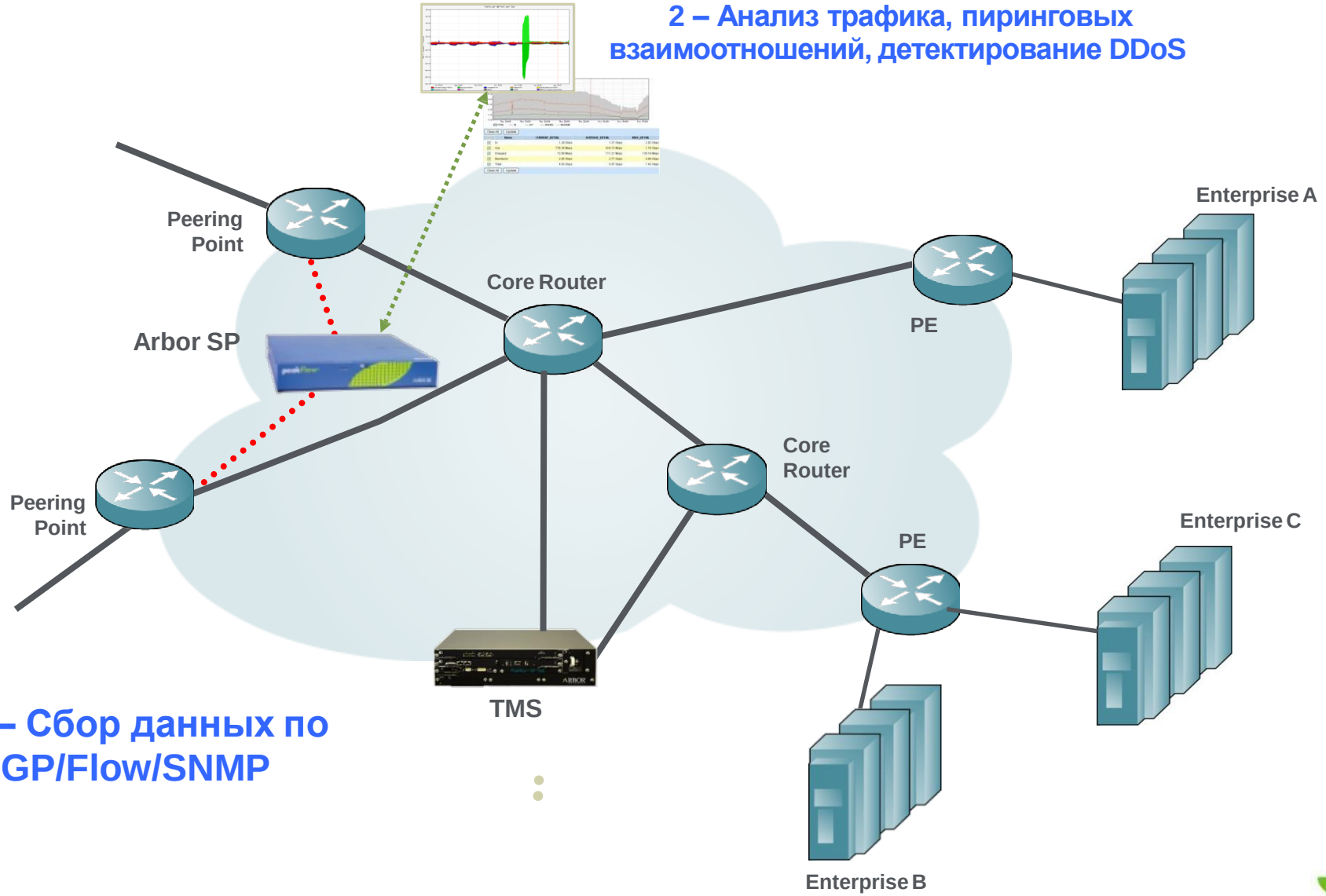
- Масштабирование объектов мониторинга
- Multihoming

Графический Интерфейс (API)

- Контроль количества одновременных сессий WEB UI
- API удобный инструмент мониторинга и экспорта информации

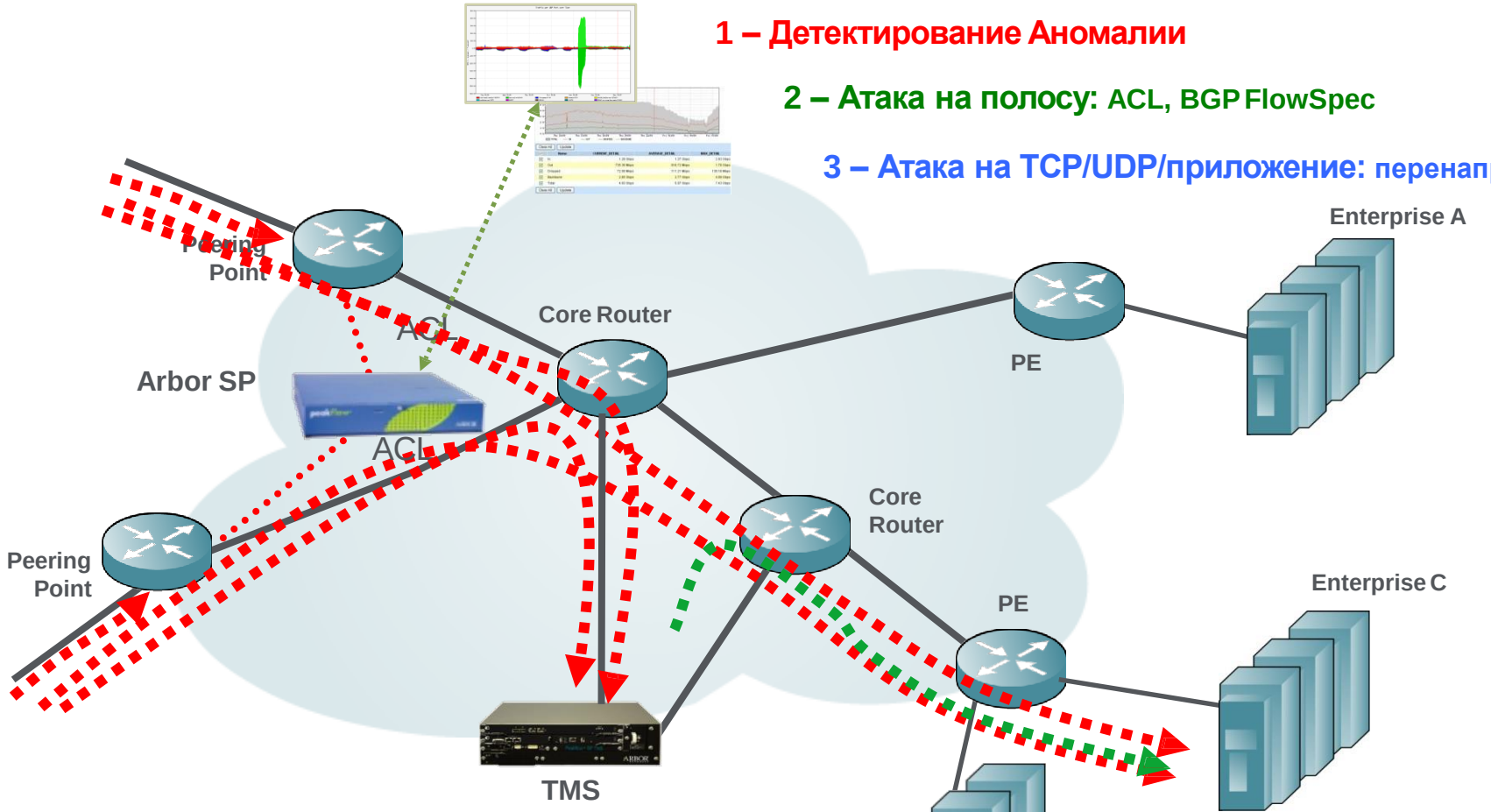


Как работает SP/TMS

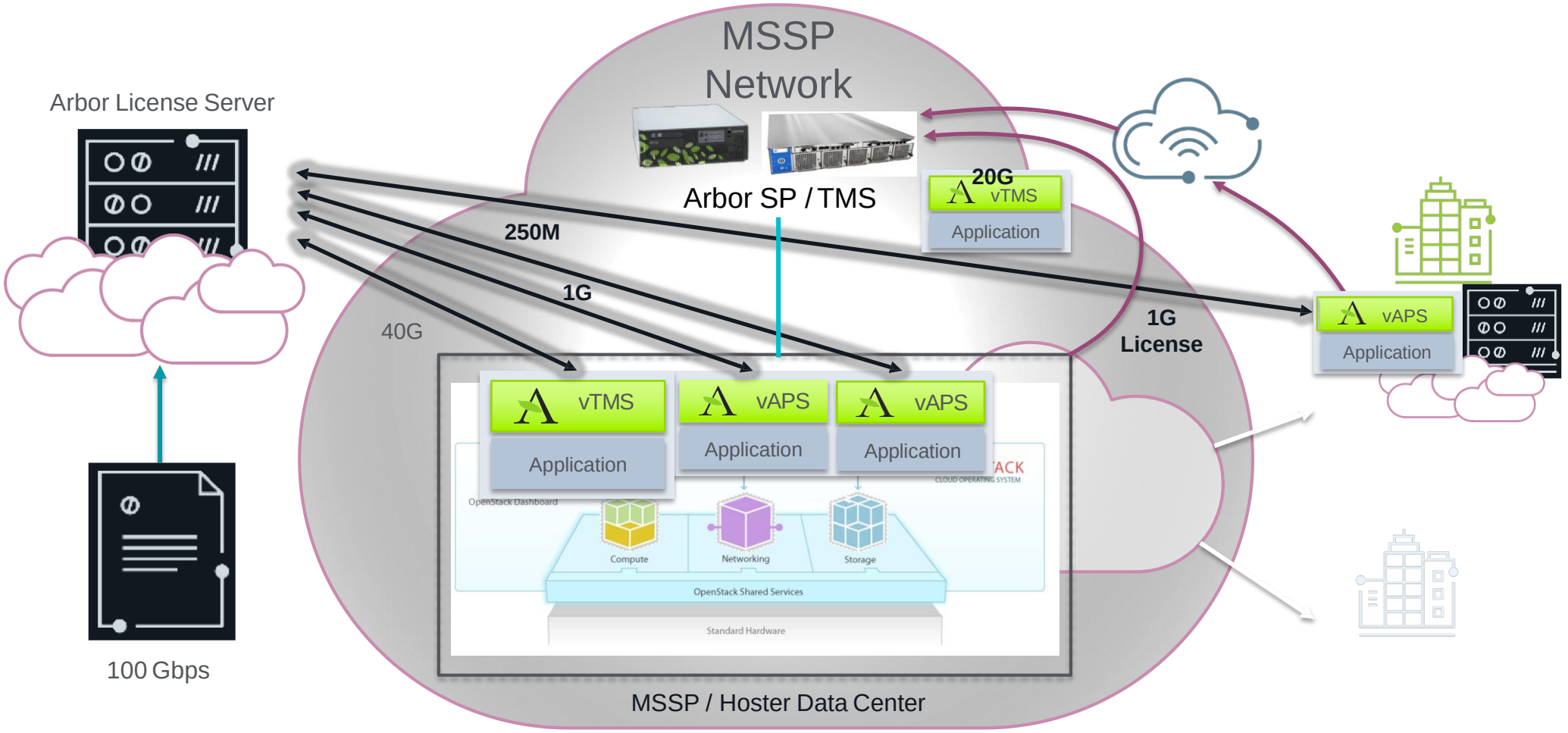


ARBOR NETWORKS

Как работает SP/TMS



vTMS licensing



Новый функционал SP/TMS

ARBOR™ NETWORKS

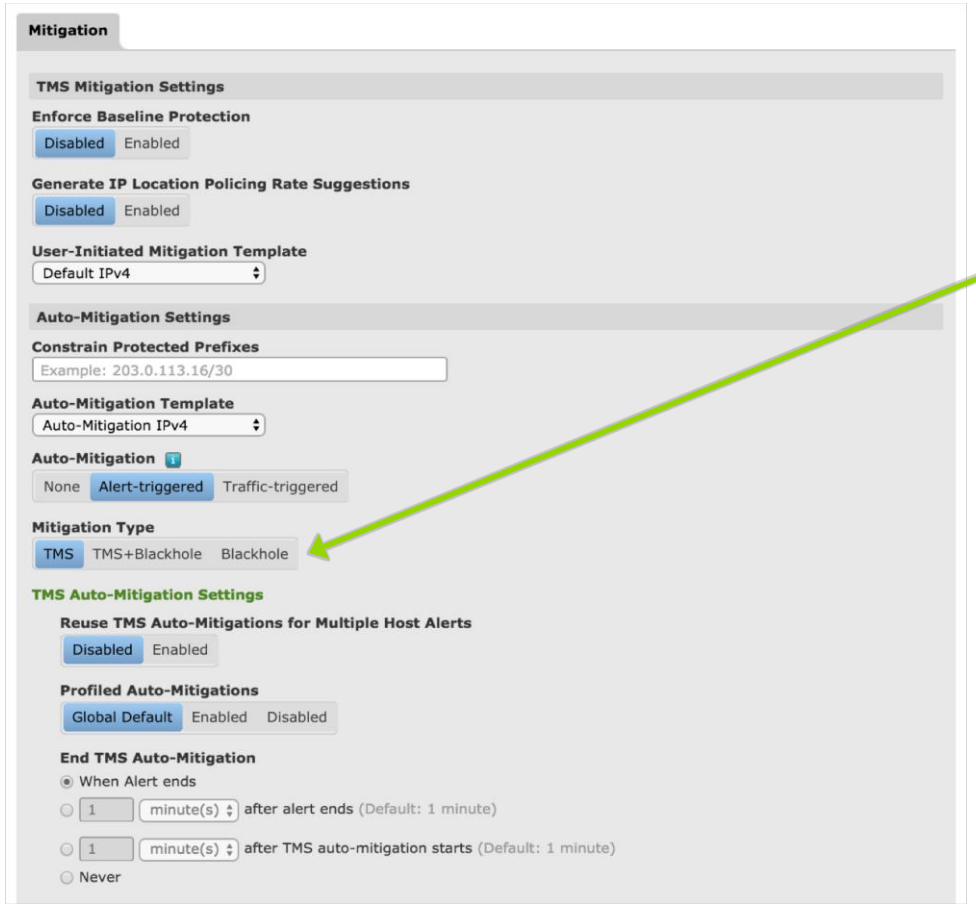
Blackhole Auto-Mitigation

8.0

- Arbor SP blackhole mitigations are designed for TMS mitigations to handle attacks until overall traffic threatens to exceed:
  - TMS capacity of customer site
  - Uplink/downlink capacity of customer site
- Arbor SP also supports blackhole mitigations as a defense for customers without TMS
  - Not surgical
  - Takes attack target offline
  - Arbor suggest that they use TMS

Blackhole Auto-Mitigation

8.0



- TMS
  - Host alert triggers TMS mitigation
- Blackhole
  - Host alert triggers blackhole mitigation
- TMS+Blackhole
  - Host alert triggers TMS mitigation
  - TMS traffic triggers blackhole mitigation

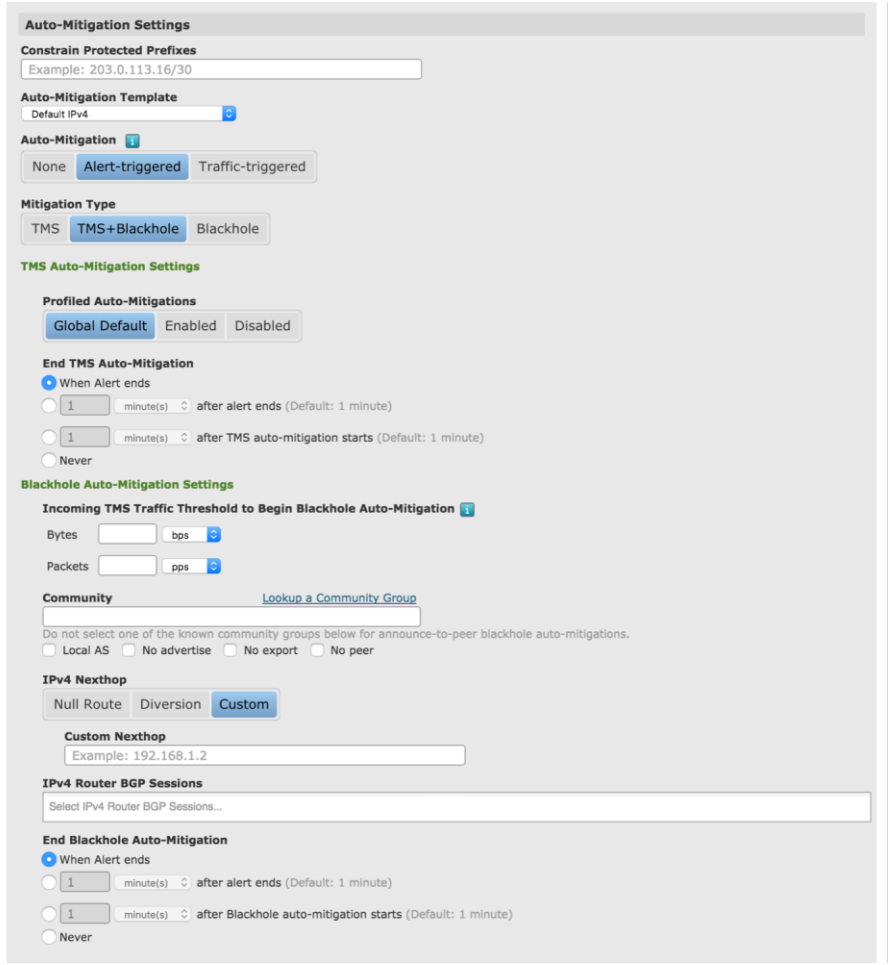
ARBOR™ NETWORKS

Blackhole Auto-Mitigation 8.0

- Each mitigation type has independent *End* settings

End TMS Auto-Mitigation conditions

End Blackhole Auto-Mitigation conditions



ARBOR NETWORKS

TMS Auto-mitigation Reuse

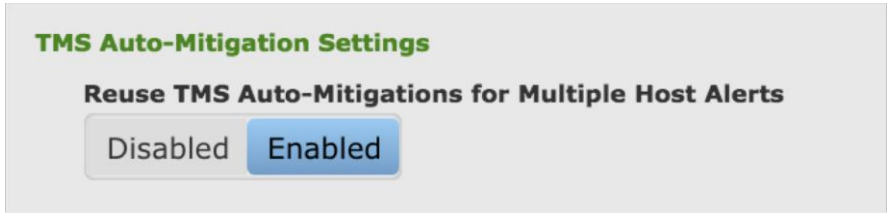
8.0

ARBOR NETWORKS

TMS Auto-mitigation Reuse

8.0

- New option to reuse an auto-mitigation for multiple host detection alerts



  - Configured per Managed Object
  - Available for alert-triggered TMS auto-mitigations only
  - **Not available for TMS+Blackhole auto-mitigations**
- Reduces the number of TMS auto-mitigations when many hosts are under simultaneous attack

ARBOR™ NETWORKS

Новые типы Host Detection

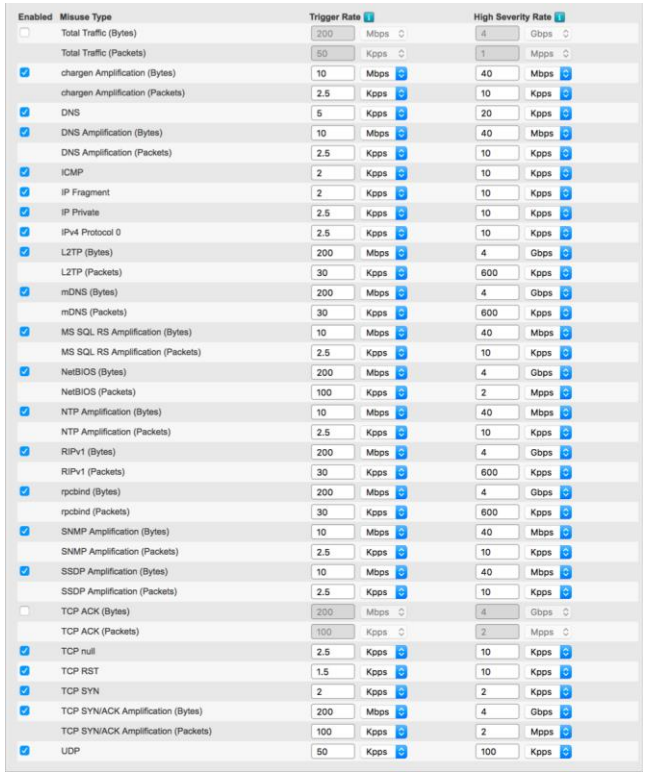
- 8.2:
  - TCP ACK
  - TCP SYN/ACK
  - L2TP
  - mDNS
  - NetBIOS
  - RIPv1
  - rpcbind
- 8.4:
  - C-LDAP
  - memcached

ARBOR™ NETWORKS

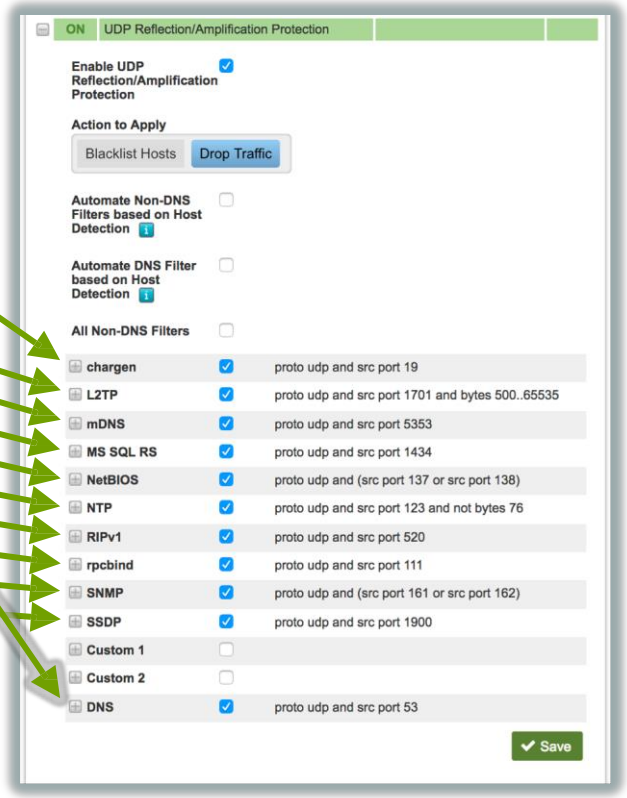
Автоматизация очистки Amplification атак

SP/TMS 8.2

Host detection settings



Enabled	Misuse Type	Trigger Rate		High Severity Rate	
☐	Total Traffic (Bytes)	200	Mbps	4	Gbps
	Total Traffic (Packets)	50	Kpps	1	Mpps
☑	chargen Amplification (Bytes)	10	Mbps	40	Mbps
	chargen Amplification (Packets)	2.5	Kpps	10	Kpps
☑	DNS	5	Kpps	20	Kpps
☑	DNS Amplification (Bytes)	10	Mbps	40	Mbps
	DNS Amplification (Packets)	2.5	Kpps	10	Kpps
☑	ICMP	2	Kpps	10	Kpps
☑	IP Fragment	2	Kpps	10	Kpps
☑	IP Private	2.5	Kpps	10	Kpps
☑	IPv4 Protocol 0	2.5	Kpps	10	Kpps
☑	L2TP (Bytes)	200	Mbps	4	Gbps
	L2TP (Packets)	30	Kpps	600	Kpps
☑	mDNS (Bytes)	200	Mbps	4	Gbps
	mDNS (Packets)	30	Kpps	600	Kpps
☑	MS SQL RS Amplification (Bytes)	10	Mbps	40	Mbps
	MS SQL RS Amplification (Packets)	2.5	Kpps	10	Kpps
☑	NetBIOS (Bytes)	200	Mbps	4	Gbps
	NetBIOS (Packets)	100	Kpps	2	Mpps
☑	NTP Amplification (Bytes)	10	Mbps	40	Mbps
	NTP Amplification (Packets)	2.5	Kpps	10	Kpps
☑	RIPv1 (Bytes)	200	Mbps	4	Gbps
	RIPv1 (Packets)	30	Kpps	600	Kpps
☑	rpcbind (Bytes)	200	Mbps	4	Gbps
	rpcbind (Packets)	30	Kpps	600	Kpps
☑	SNMP Amplification (Bytes)	10	Mbps	40	Mbps
	SNMP Amplification (Packets)	2.5	Kpps	10	Kpps
☑	SSDP Amplification (Bytes)	10	Mbps	40	Mbps
	SSDP Amplification (Packets)	2.5	Kpps	10	Kpps
☐	TCP ACK (Bytes)	200	Mbps	4	Gbps
	TCP ACK (Packets)	100	Kpps	2	Mpps
☑	TCP null	2.5	Kpps	10	Kpps
☑	TCP RST	1.5	Kpps	10	Kpps
☑	TCP SYN	2	Kpps	2	Kpps
☑	TCP SYN/ACK Amplification (Bytes)	200	Mbps	4	Gbps
	TCP SYN/ACK Amplification (Packets)	100	Kpps	2	Mpps
☑	UDP	50	Kpps	100	Kpps

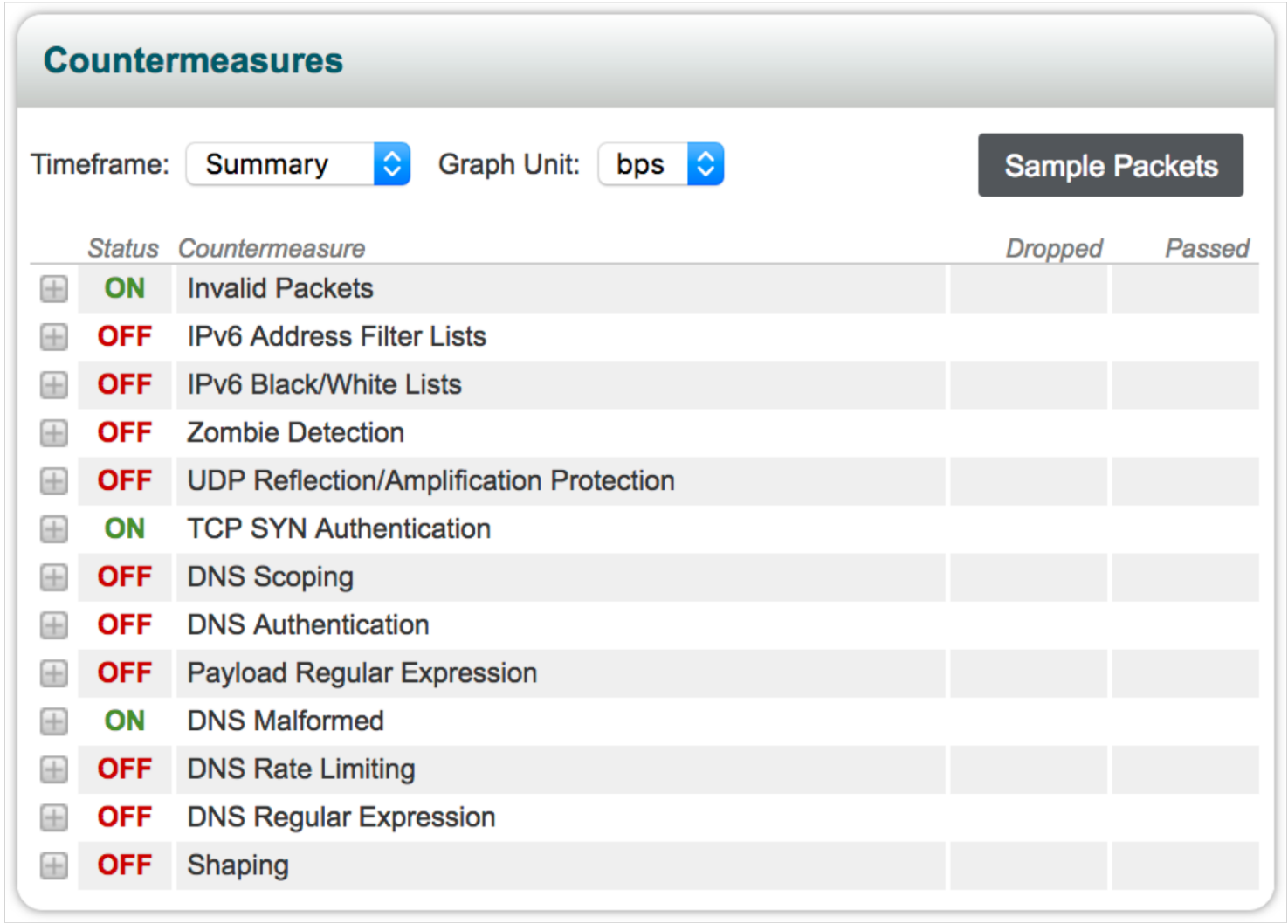


TMS mitigation settings

ARBOR NETWORKS

DNS IPv6 противомеры

SP/TMS 8.2

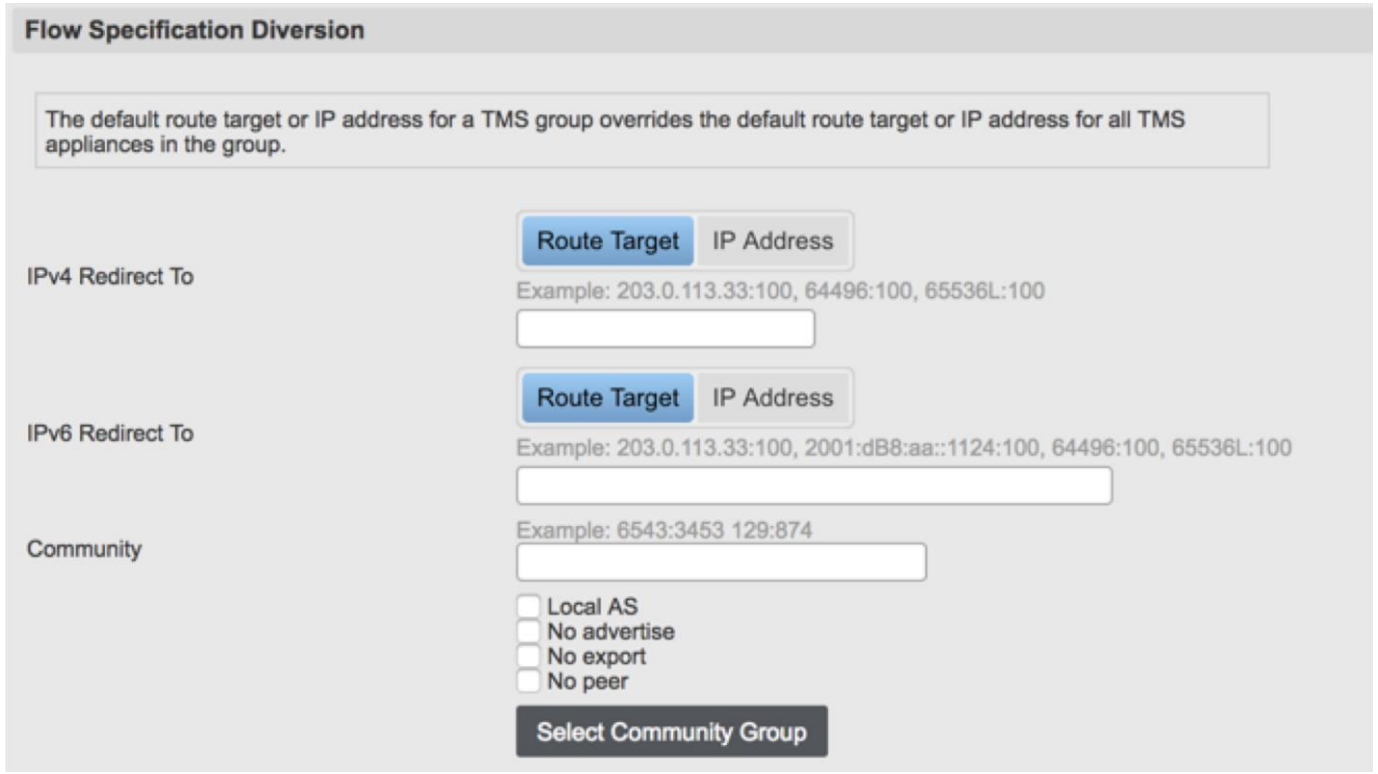


ARBOR™ NETWORKS

Redirect IPv4/IPv6 с помощью FlowSpec

SP 8.1/8.3

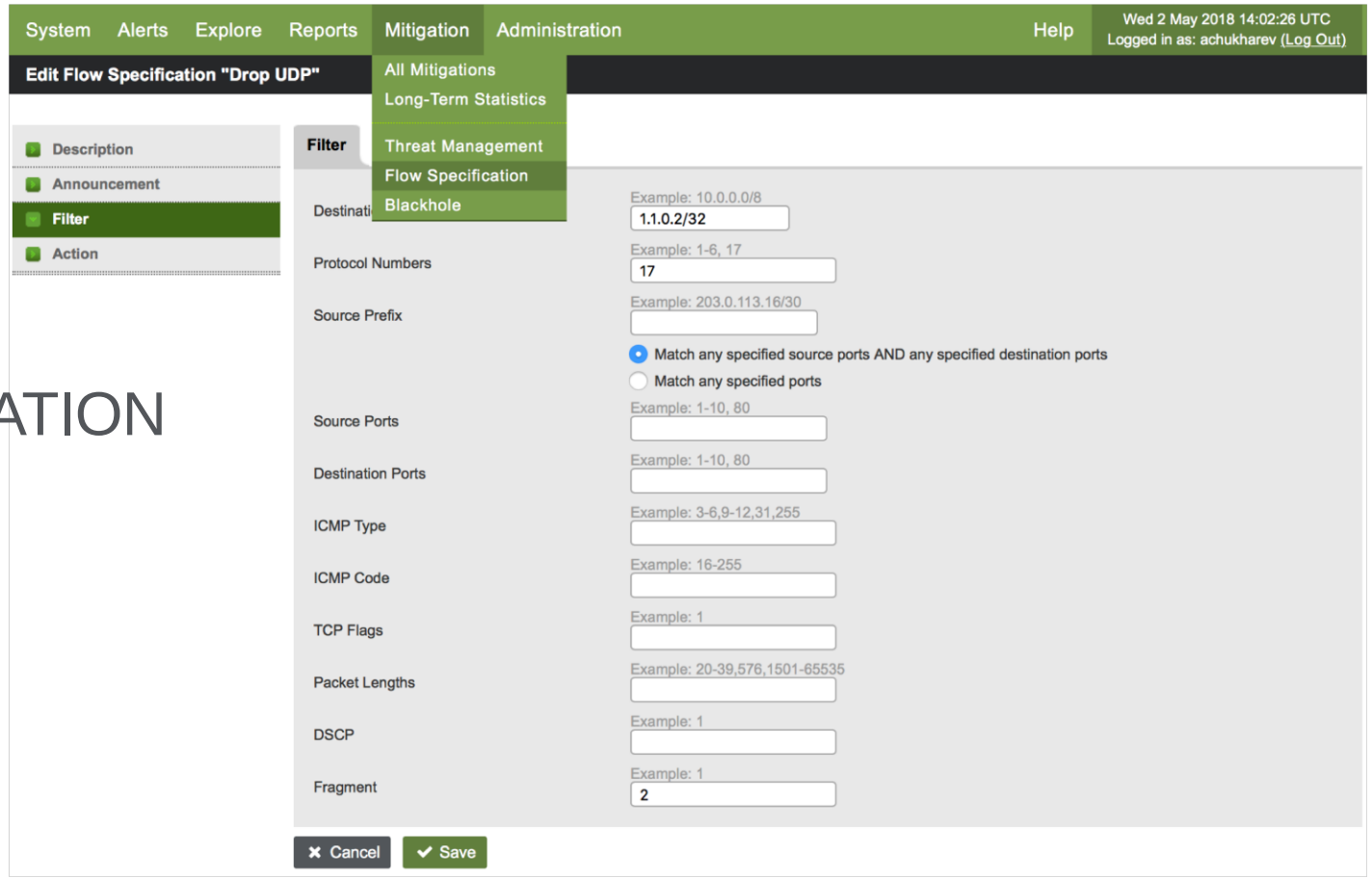
- TMS IPv4/IPv6 mitigations support flowspec diversion to TMS
  - Only with diversion via SP peering announcements
- Redirect traffic to route target or an IPv4/IPv6 address
- Feature parity with IPv4 flowspec diversion to TMS

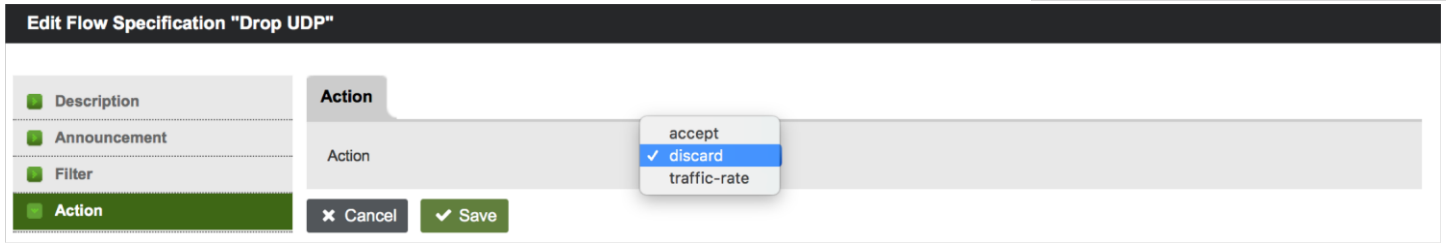


ARBOR NETWORKS

FlowSpec offload

- Makes the router a part of MITIGATION system
- Offload FlowSpec filters to router
- Blocks BULK traffic

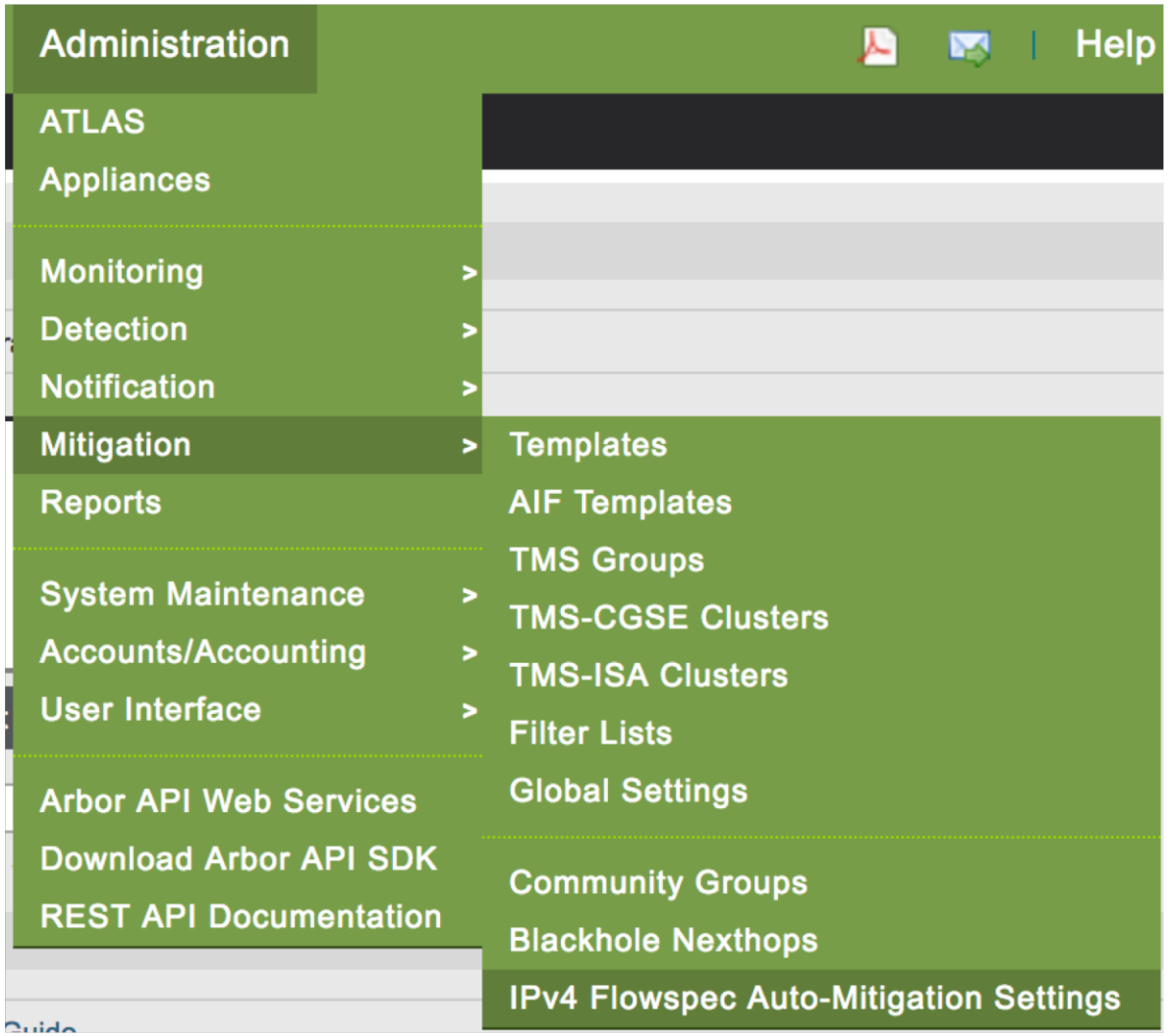


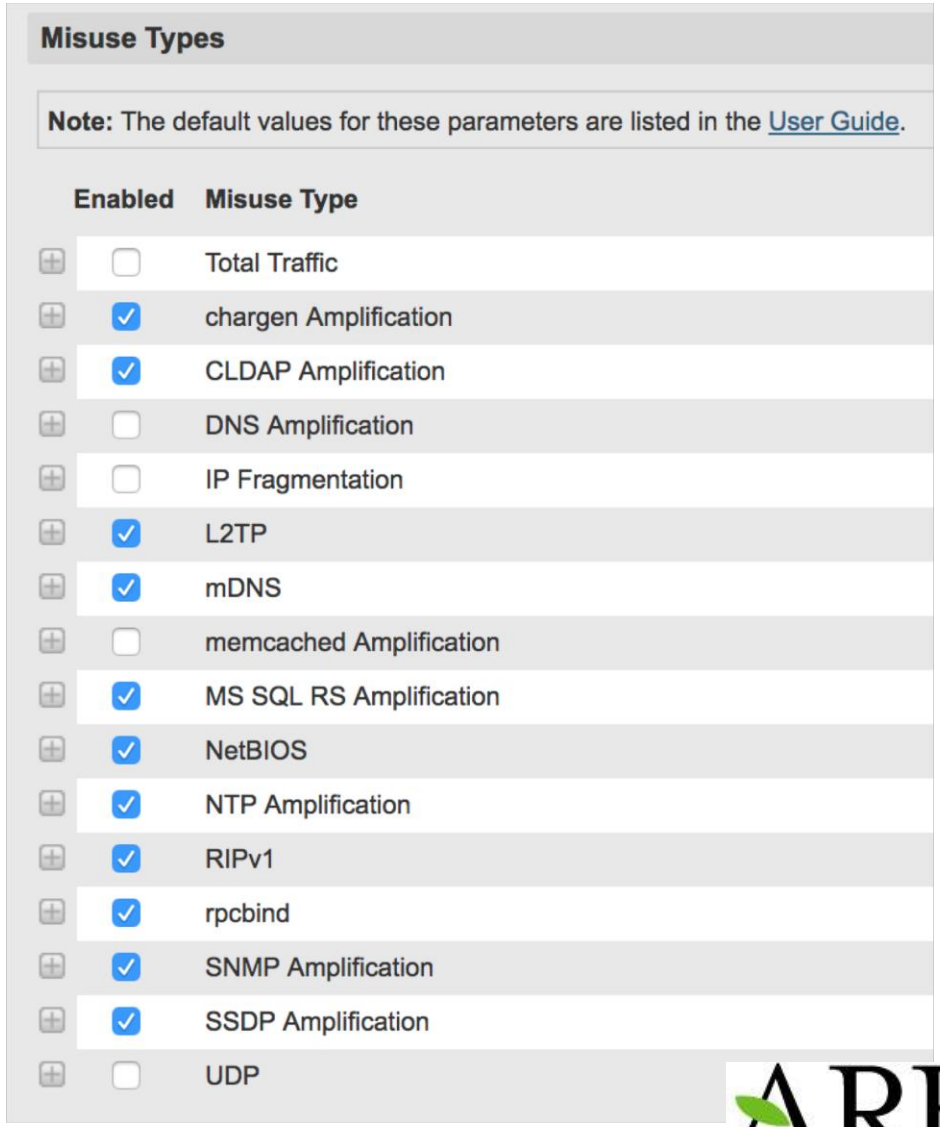


ARBOR NETWORKS

FlowSpec Automitigation

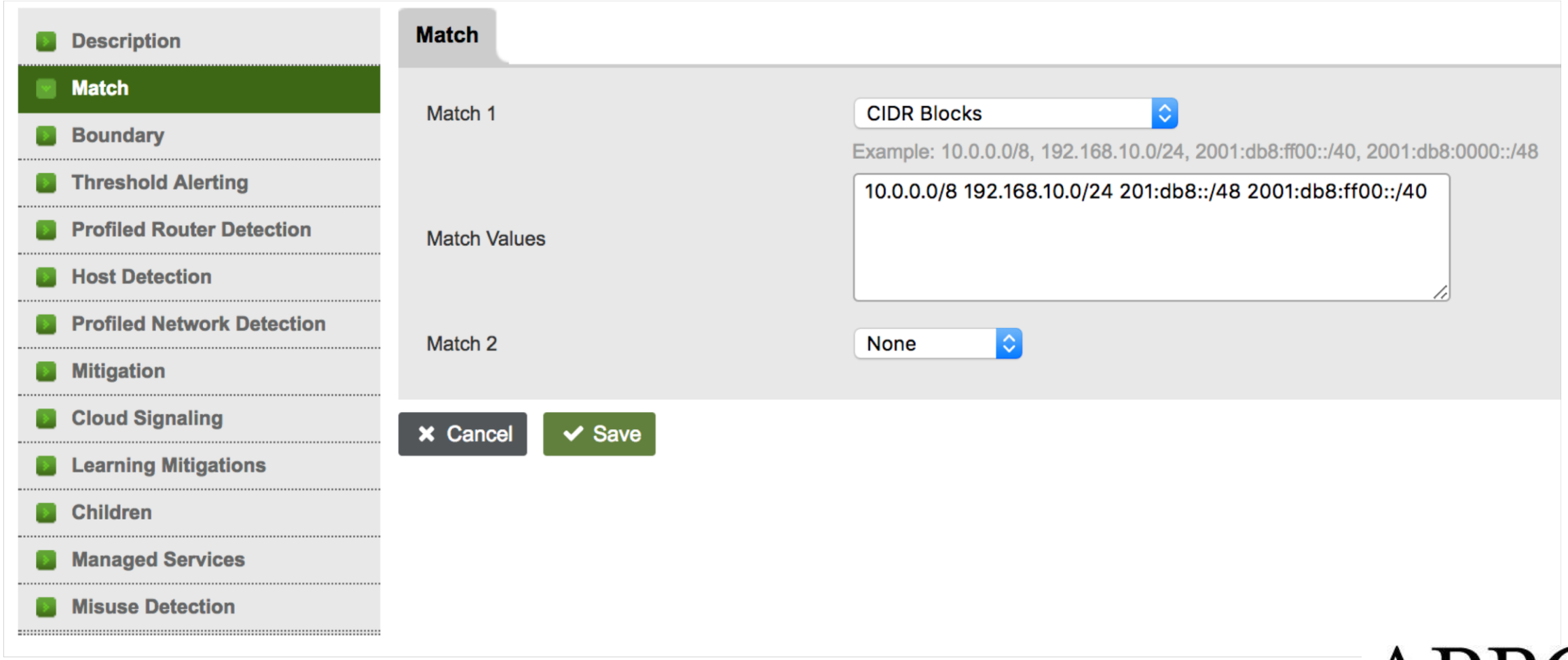
SP 8.4





IPv4/IPv6 комбинированные MO

SP 8.4

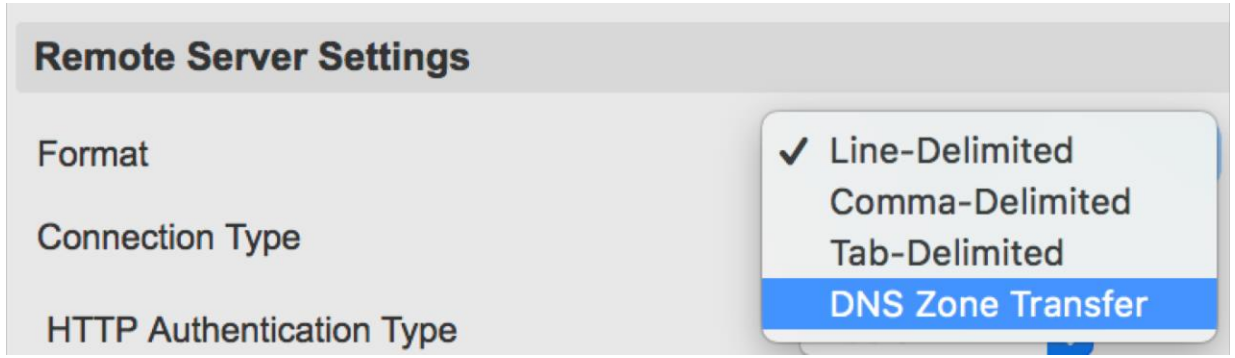


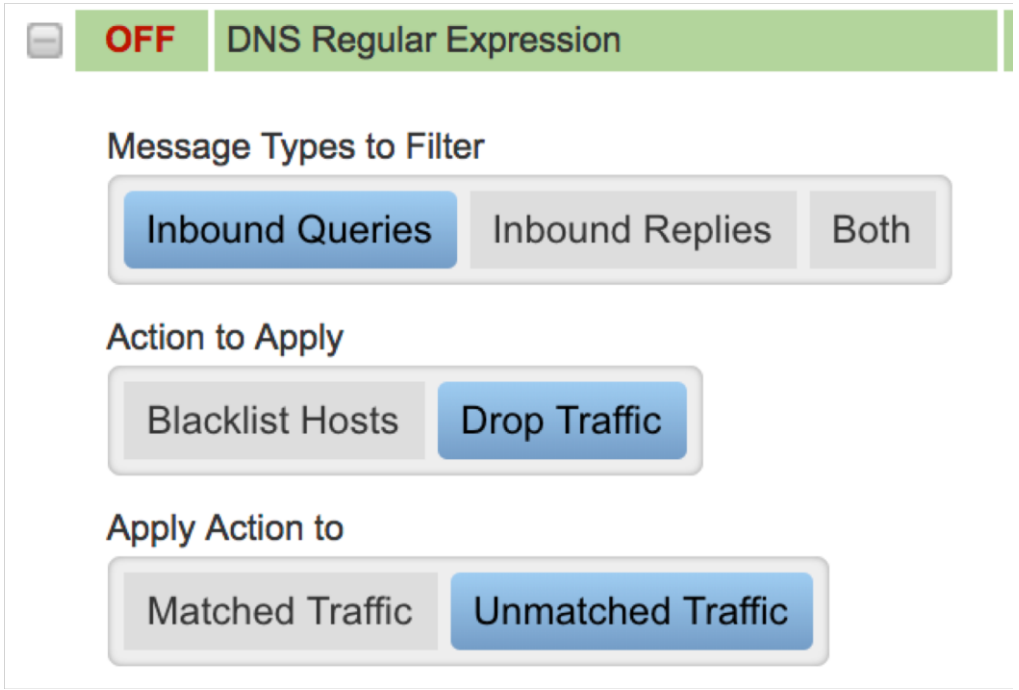
ARBOR NETWORKS

Защита авторитативных DNS серверов

SP/TMS 8.4

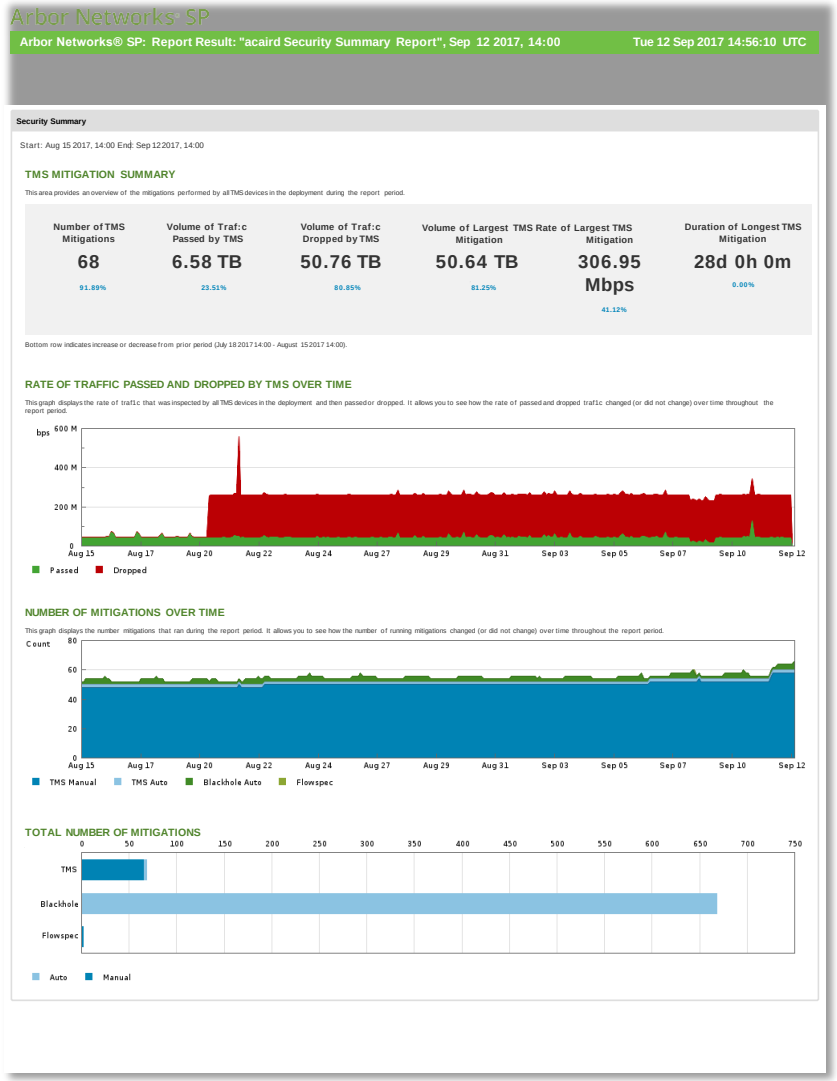
- SP выполняет Zone Transfer и создает/обновляет DNS whitelist, который применяется в mitigation.

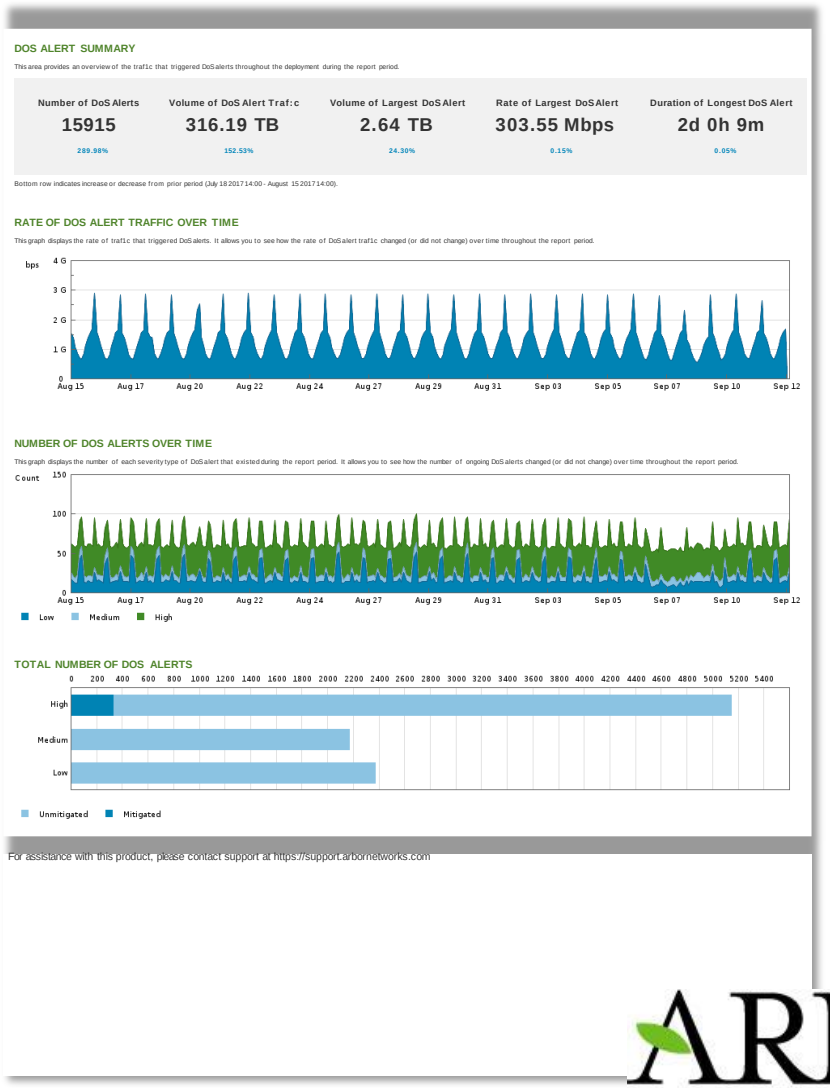




ARBOR NETWORKS

Executive reports





ARBOR™ NETWORKS

Atlas Global DDoS Report

- Atlas Global DDoS Report
  - Глобальное состояние мира DDoS за последний месяц
  - Создается ASERT
  - Данные из ATLAS

ARBOR NETWORKS