

Arbor Networks

Продуктовая линейка SP/TMS

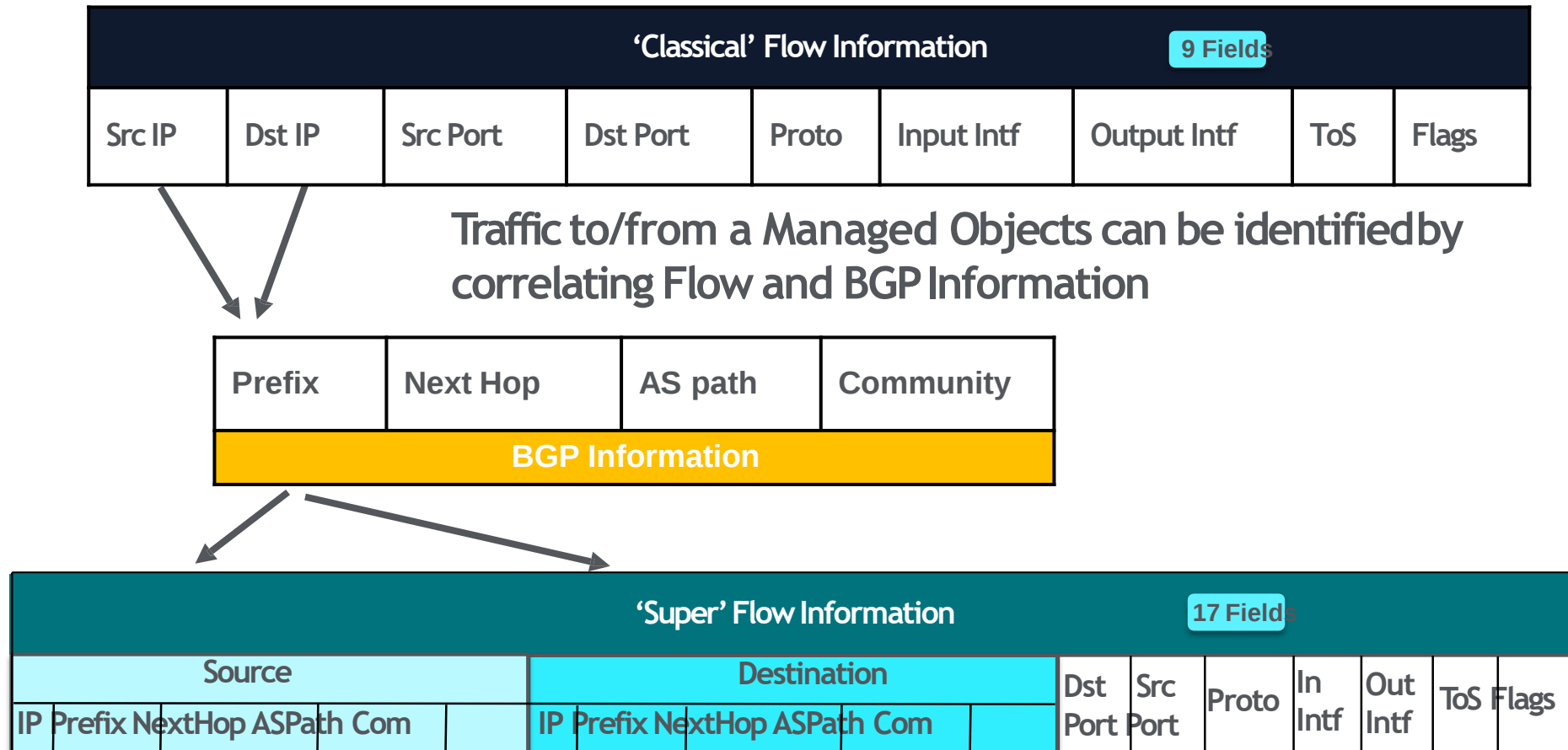
Визуализация – Знай свою сеть



- 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?

Насыщение FLOW

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



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

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

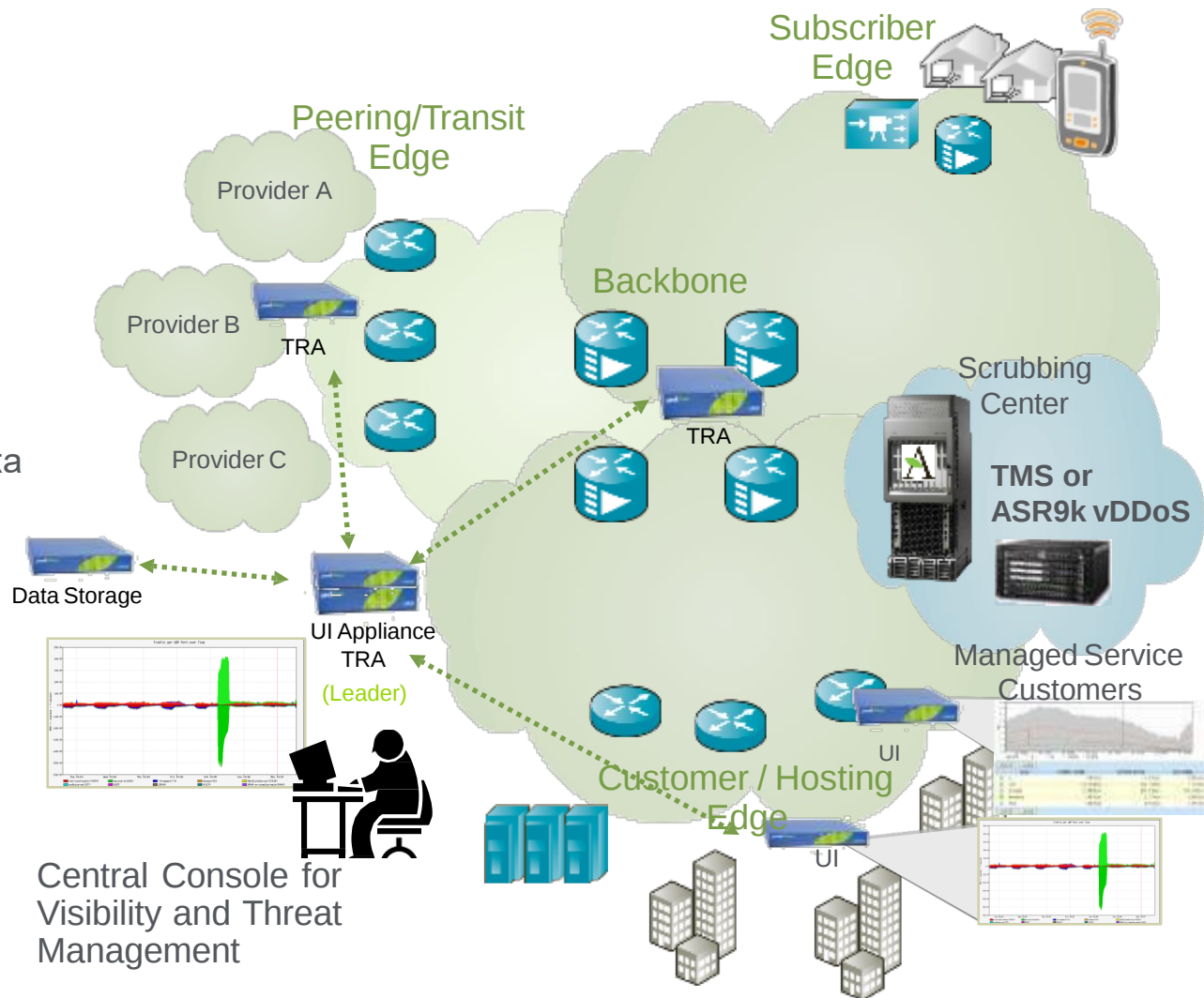
“Хирургическое” выделение зловредного трафика

Объекты мониторинга

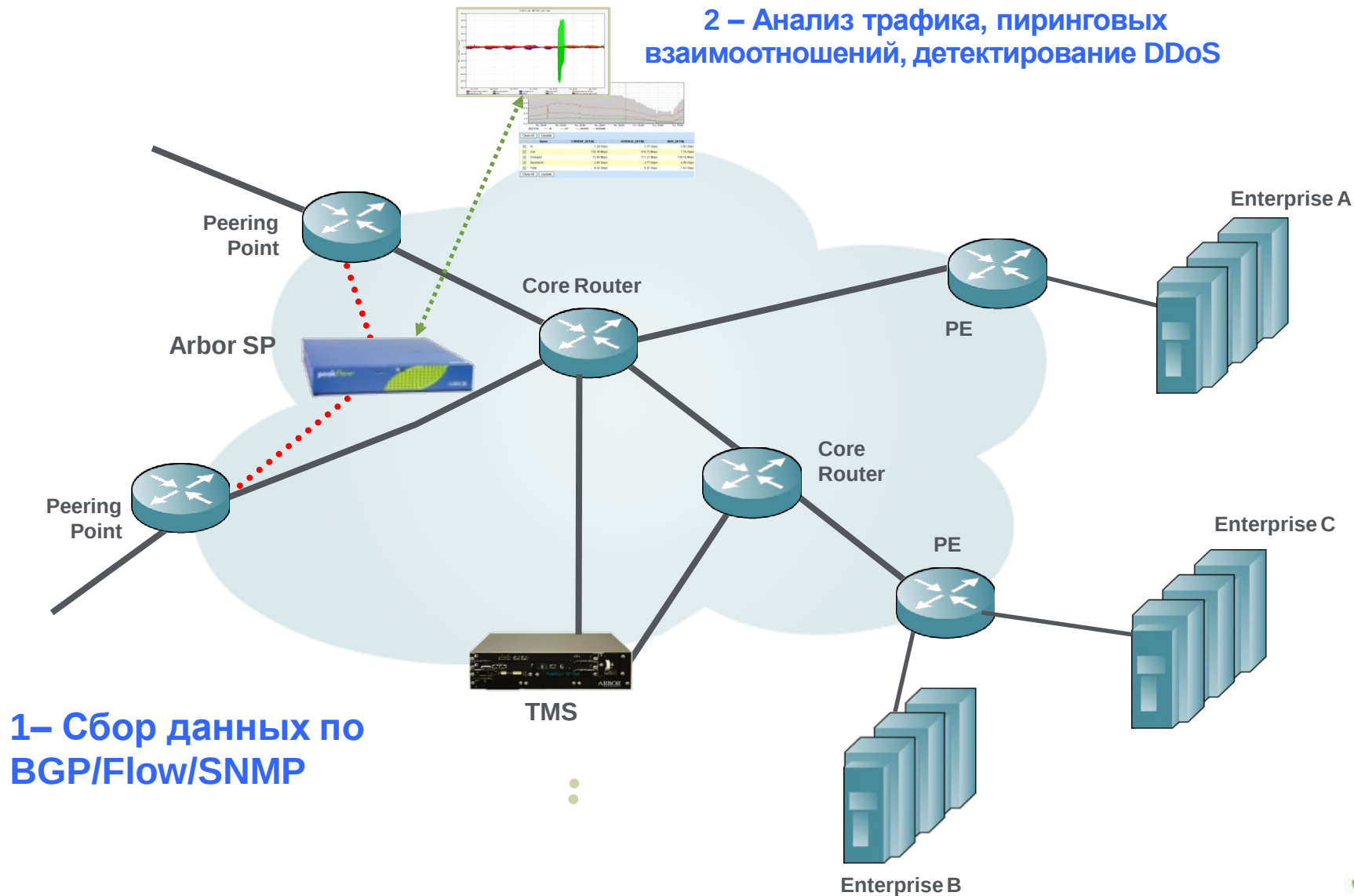
- Масштабирование объектов мониторинга
- Multihoming

Графический Интерфейс (API)

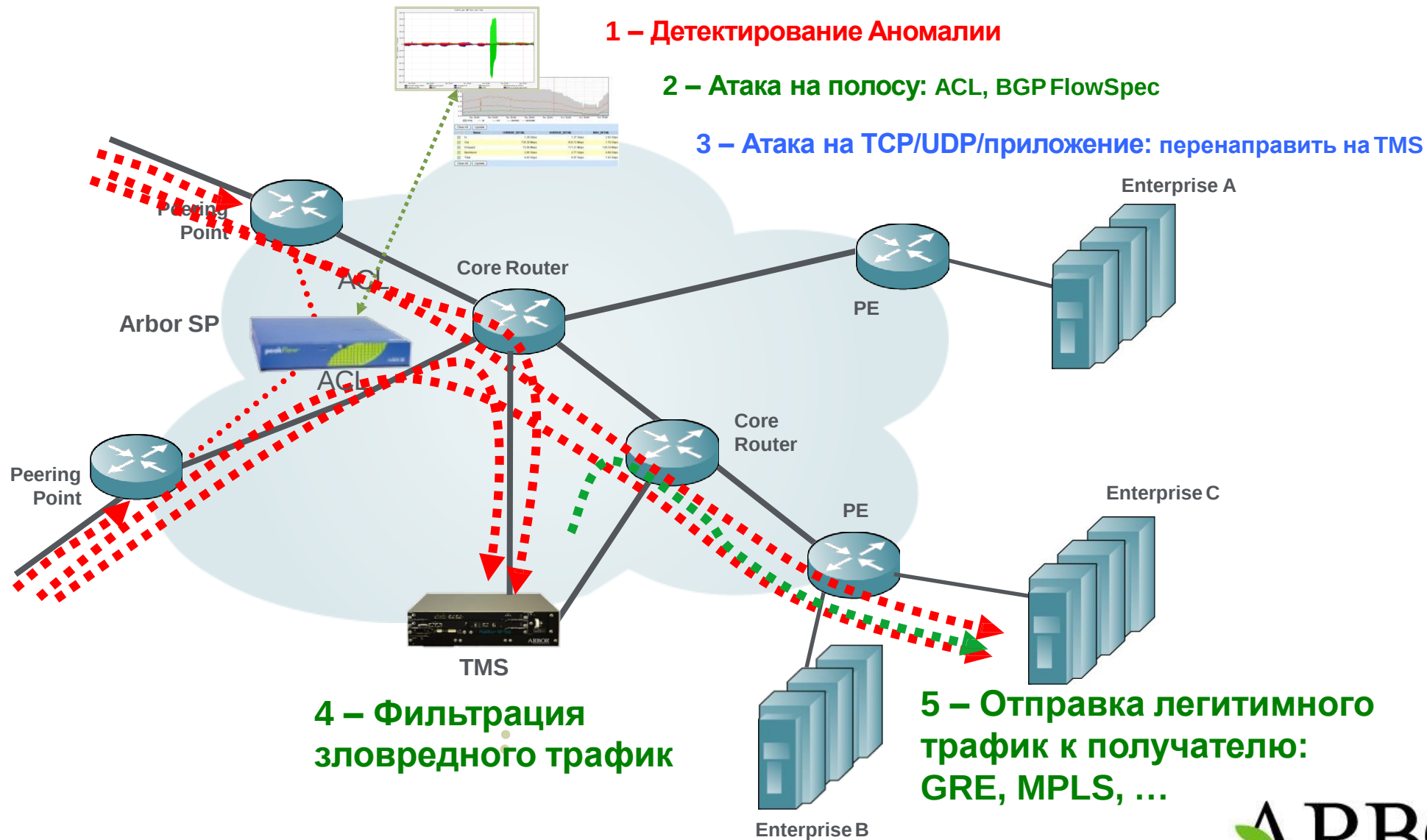
- Контроль количества одновременных сессий WEB UI
- API удобный инструмент мониторинга и экспорта информации



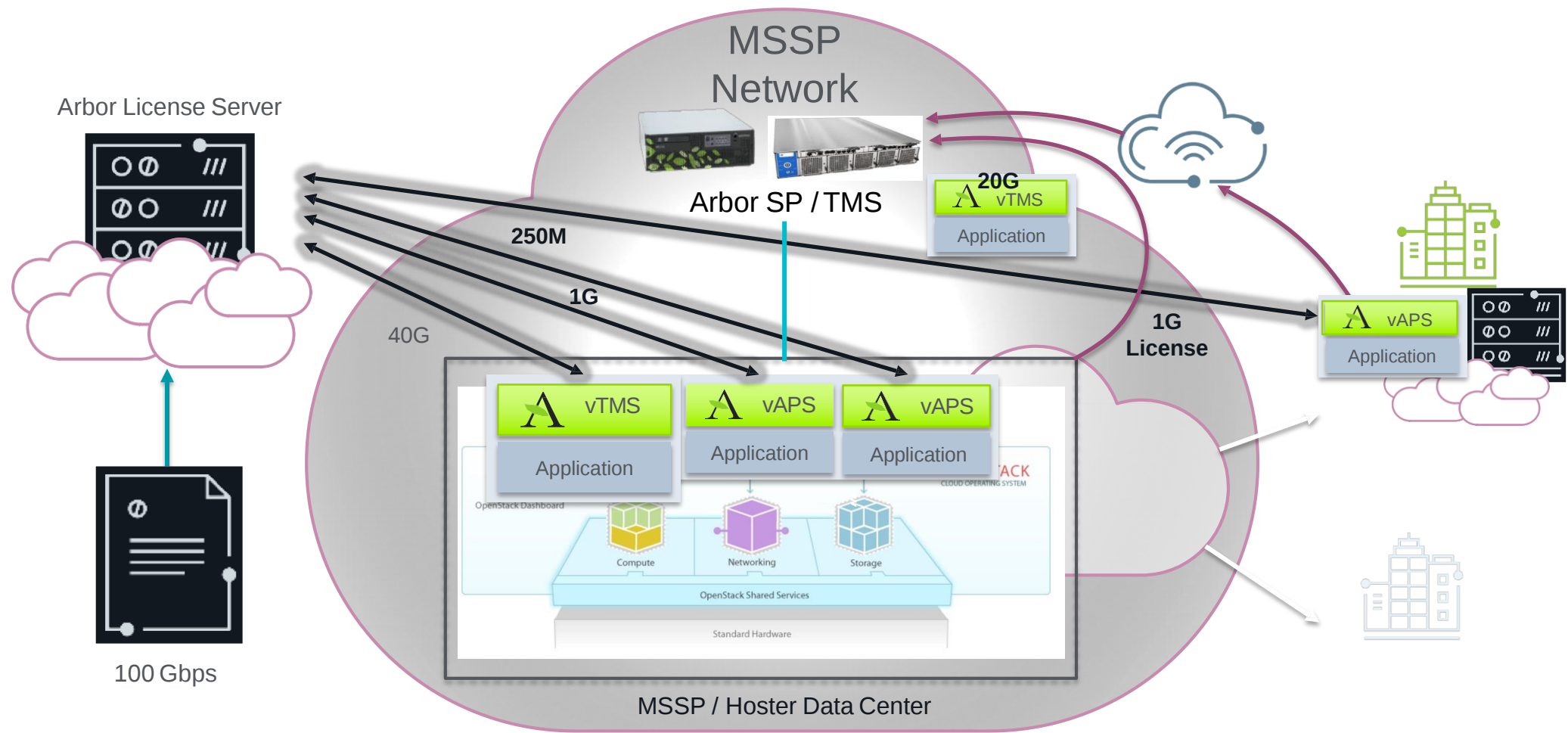
Как работает SP/TMS



Как работает SP/TMS



vTMS licensing



Новый функционал SP/TMS

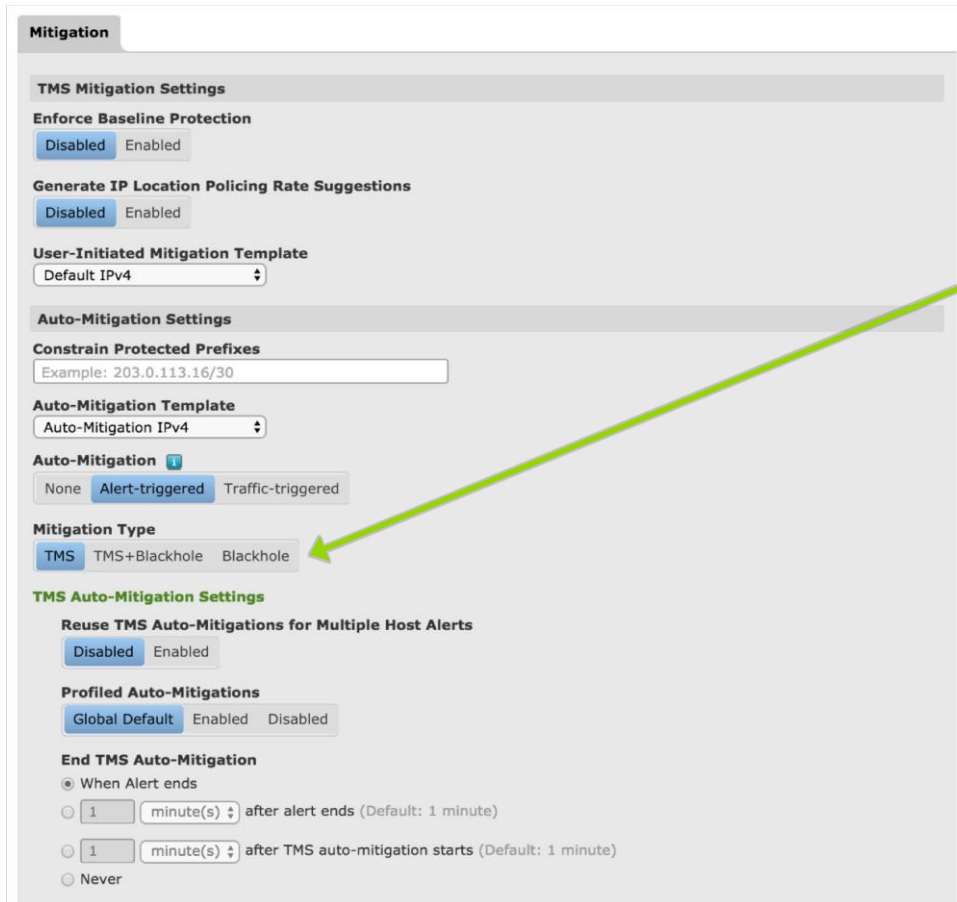
Blackhole Auto-Mitigation

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



Mitigation

TMS Mitigation Settings

Enforce Baseline Protection

Generate IP Location Policing Rate Suggestions

User-Initiated Mitigation Template
Default IPv4

Auto-Mitigation Settings

Constrain Protected Prefixes
Example: 203.0.113.16/30

Auto-Mitigation Template
Auto-Mitigation IPv4

Auto-Mitigation ⓘ

Mitigation Type
 ←

TMS Auto-Mitigation Settings

Reuse TMS Auto-Mitigations for Multiple Host Alerts

Profiled Auto-Mitigations

End TMS Auto-Mitigation
☒ When Alert ends
☐ 1 minute(s) after alert ends (Default: 1 minute)
☐ 1 minute(s) after TMS auto-mitigation starts (Default: 1 minute)
☐ Never

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

Blackhole Auto-Mitigation

8.0

- Each mitigation type has independent *End* settings

End TMS Auto-Mitigation conditions

End Blackhole Auto-Mitigation conditions

The screenshot displays the 'Auto-Mitigation Settings' configuration page. It includes sections for 'Constrain Protected Prefixes', 'Auto-Mitigation Template', 'Auto-Mitigation' (with 'Alert-triggered' selected), 'Mitigation Type' (with 'TMS+Blackhole' selected), 'TMS Auto-Mitigation Settings' (with 'Global Default' selected), 'End TMS Auto-Mitigation' (with 'When Alert ends' selected), 'Blackhole Auto-Mitigation Settings' (with 'Incoming TMS Traffic Threshold to Begin Blackhole Auto-Mitigation' selected), 'Community' (with 'Local AS' selected), 'IPv4 Nexthop' (with 'Custom' selected), and 'IPv4 Router BGP Sessions'.

TMS Auto-mitigation Reuse

8.0

Edit Appliance "anchor"

Appliance

SNMP

Deployment

ArborFlow

Patch Panel

Subinterfaces

Ports

IPv4 GRE

IPv6 GRE

Advanced

Advanced

Maximum Ongoing Mitigations

Lowering the maximum number of ongoing mitigations allows more state to be kept per mitigation.

⚠ CAUTION:

Changing this setting briefly interrupts packet processing while SP reconfigures the TMS appliance. Arbor recommends that you only change this setting when there are no running mitigations.

Maximum Ongoing Mitigations

(Default: 50)

50

Range: 10 - 100

Hardware Blacklisting

Block on

Source

Source+Mitigation

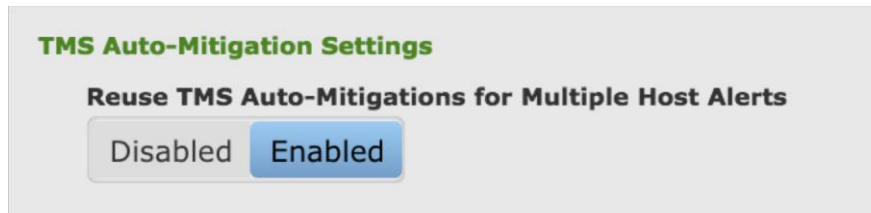
Cancel

Save

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

Новые типы Host Detection

- 8.2:

- TCPACK
- TCP SYN/ACK
- L2TP
- mDNS
- NetBIOS
- RIPv1
- rpcbind

- 8.4:

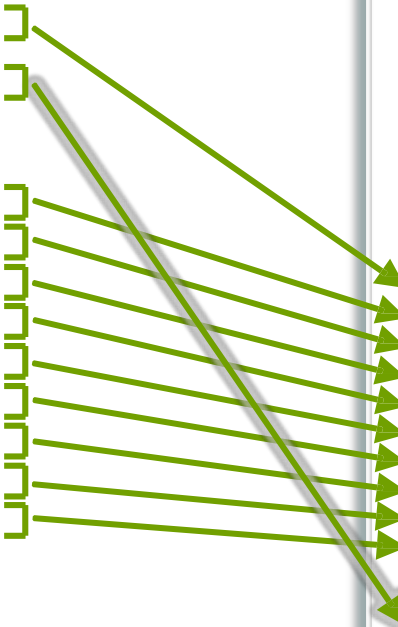
- C-LDAP
- memcached

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

ON

UDP Reflection/Amplification Protection

Enable UDP Reflection/Amplification Protection

☒

Action to Apply

Blacklist Hosts

Drop Traffic

Automate Non-DNS Filters based on Host Detection

☐

Automate DNS Filter based on Host Detection

☐

All Non-DNS Filters

☐

chargen

☒

proto udp and src port 19

L2TP

☒

proto udp and src port 1701 and bytes 500..65535

mDNS

☒

proto udp and src port 5353

MS SQL RS

☒

proto udp and src port 1434

NetBIOS

☒

proto udp and (src port 137 or src port 138)

NTP

☒

proto udp and src port 123 and not bytes 76

RIPv1

☒

proto udp and src port 520

rpcbind

☒

proto udp and src port 111

SNMP

☒

proto udp and (src port 161 or src port 162)

SSDP

☒

proto udp and src port 1900

Custom 1

☐

Custom 2

☐

DNS

☒

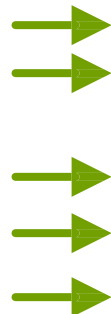
proto udp and src port 53

Save

DNS IPv6 противомеры

SP/TMS 8.2

Countermeasures				
Timeframe:		Summary	Graph Unit:	bps
			Sample Packets	
	Status	Countermeasure	Dropped	Passed
	ON	Invalid Packets		
	OFF	IPv6 Address Filter Lists		
	OFF	IPv6 Black/White Lists		
	OFF	Zombie Detection		
	OFF	UDP Reflection/Amplification Protection		
	ON	TCP SYN Authentication		
	OFF	DNS Scoping		
	OFF	DNS Authentication		
	OFF	Payload Regular Expression		
	ON	DNS Malformed		
	OFF	DNS Rate Limiting		
	OFF	DNS Regular Expression		
	OFF	Shaping		



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

Flow Specification Diversion

The default route target or IP address for a TMS group overrides the default route target or IP address for all TMS appliances in the group.

IPv4 Redirect To

Example: 203.0.113.33:100, 64496:100, 65536L:100

IPv6 Redirect To

Example: 203.0.113.33:100, 2001:db8:aa::1124:100, 64496:100, 65536L:100

Community

Example: 6543:3453 129:874

☐ Local AS
☐ No advertise
☐ No export
☐ No peer

FlowSpec offload

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

System Alerts Explore Reports Mitigation Administration Help Wed 2 May 2018 14:02:26 UTC
Logged in as: achukharev (Log Out)

Edit Flow Specification "Drop UDP"

Filter

Destination: 1.1.0.2/32

Protocol Numbers: 17

Source Prefix:

Source Ports:

Destination Ports:

ICMP Type:

ICMP Code:

TCP Flags:

Packet Lengths:

DSCP:

Fragment: 2

Match any specified source ports AND any specified destination ports

Match any specified ports

Cancel Save

Edit Flow Specification "Drop UDP"

Action

accept

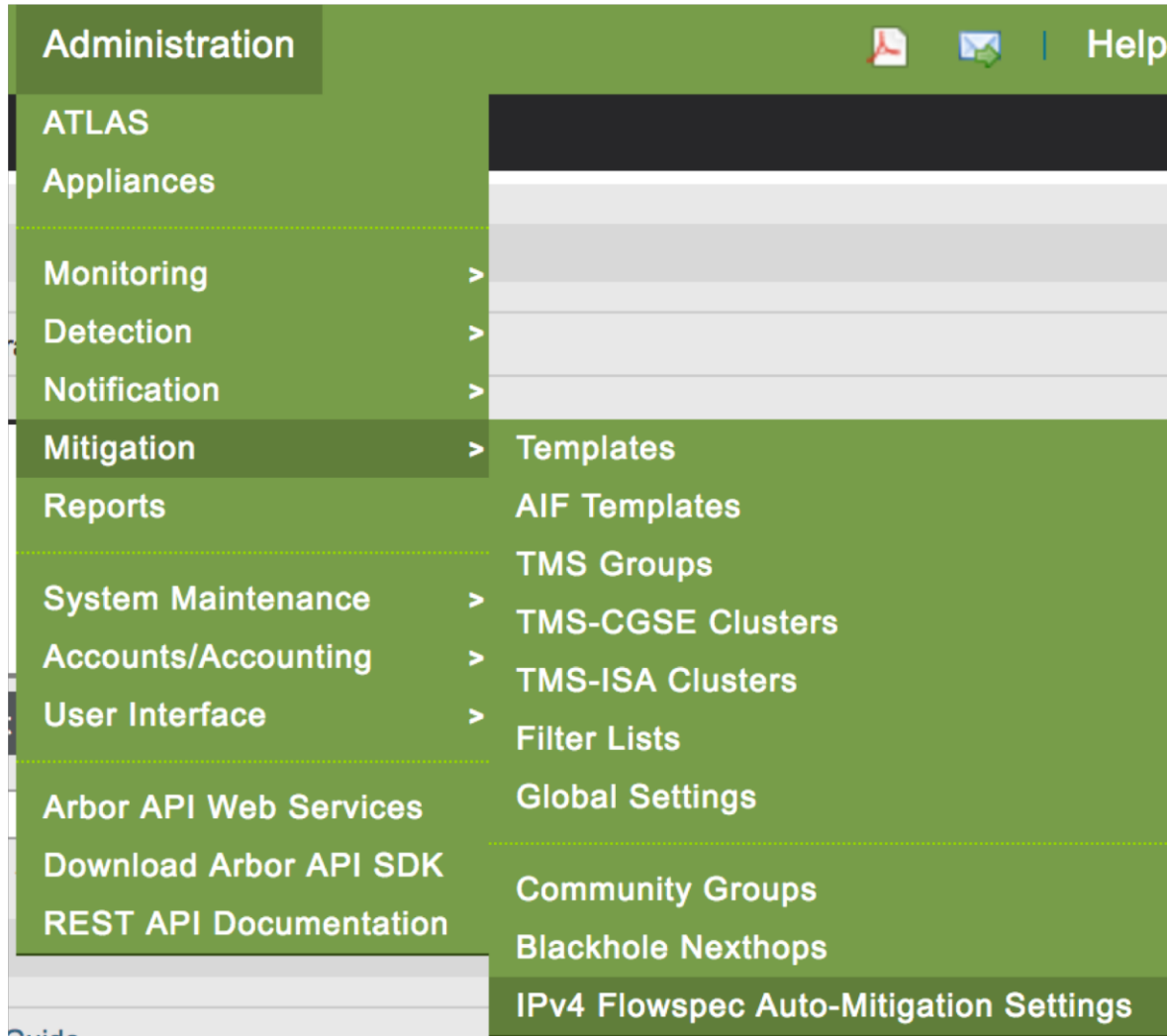
✓ discard

traffic-rate

Cancel Save

FlowSpec Automitigation

SP 8.4



Misuse Types		
Note: The default values for these parameters are listed in the User Guide .		
Enabled	Misuse Type	
	☐	Total Traffic
	☒	chargen Amplification
	☒	CLDAP Amplification
	☐	DNS Amplification
	☐	IP Fragmentation
	☒	L2TP
	☒	mDNS
	☐	memcached Amplification
	☒	MS SQL RS Amplification
	☒	NetBIOS
	☒	NTP Amplification
	☒	RIPv1
	☒	rpcbind
	☒	SNMP Amplification
	☒	SSDP Amplification
	☐	UDP

IPv4/IPv6 комбинированные МО

SP 8.4

Description

Match

Boundary

Threshold Alerting

Profiled Router Detection

Host Detection

Profiled Network Detection

Mitigation

Cloud Signaling

Learning Mitigations

Children

Managed Services

Misuse Detection

Match

Match 1

CIDR Blocks

Example: 10.0.0.0/8, 192.168.10.0/24, 2001:db8:ff00::/40, 2001:db8:0000::/48

10.0.0.0/8 192.168.10.0/24 201:db8::/48 2001:db8:ff00::/40

Match Values

Match 2

None

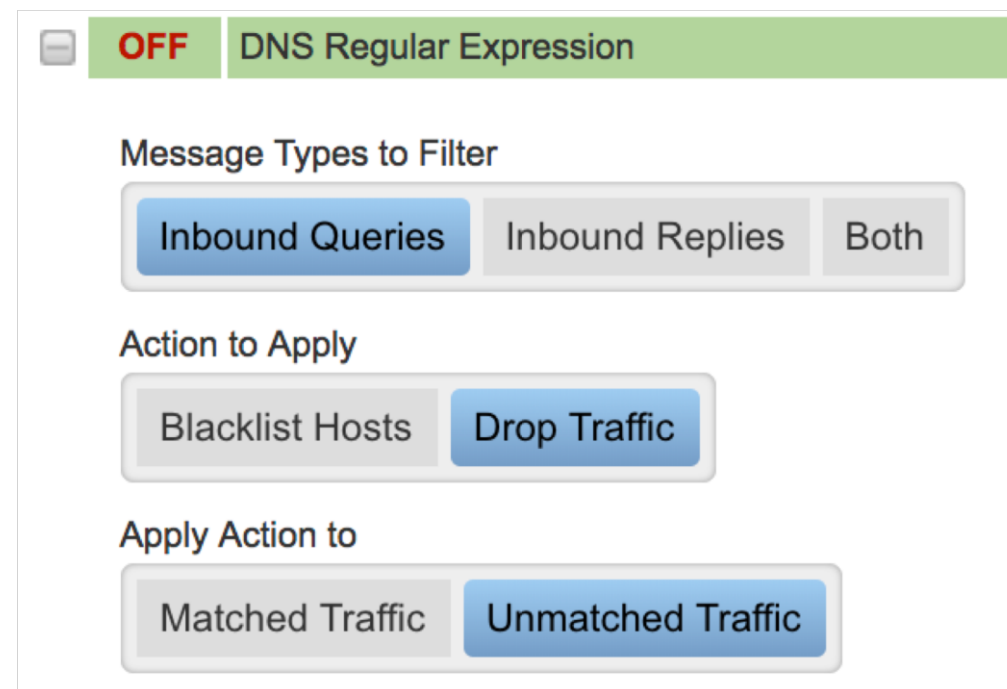
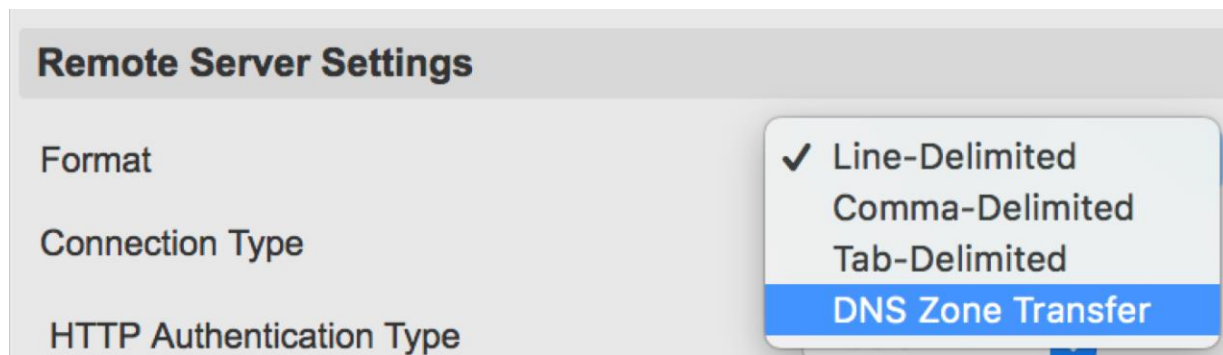
Cancel

Save

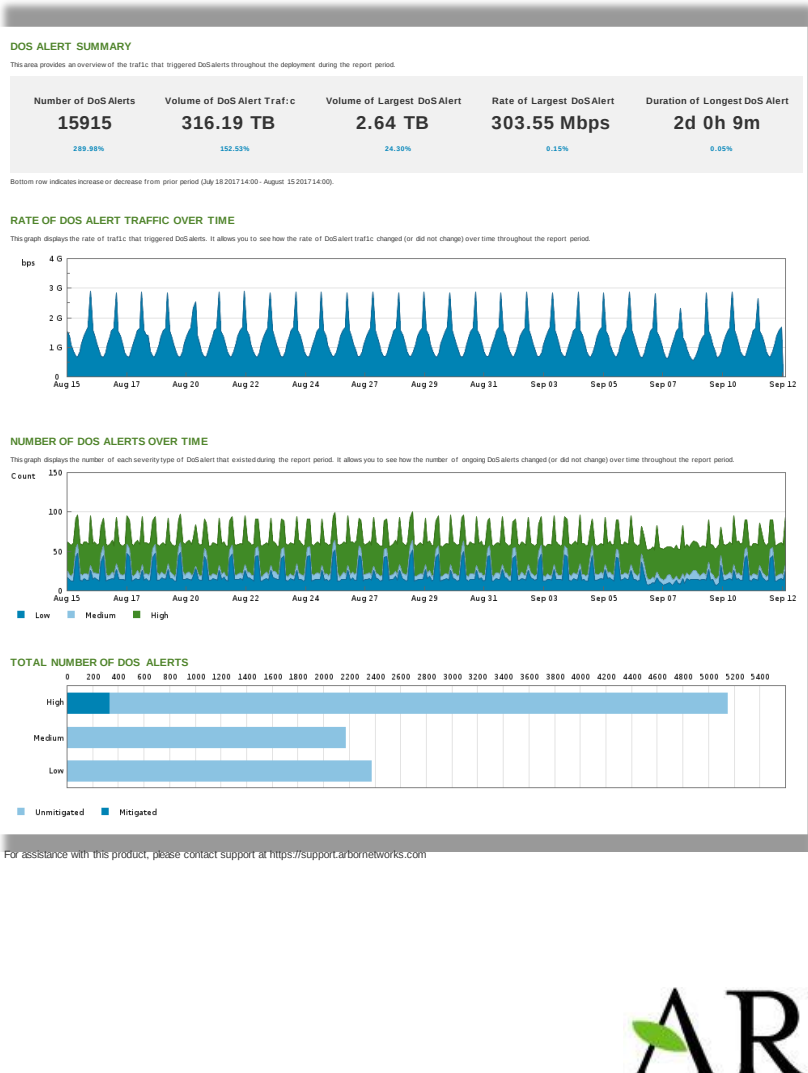
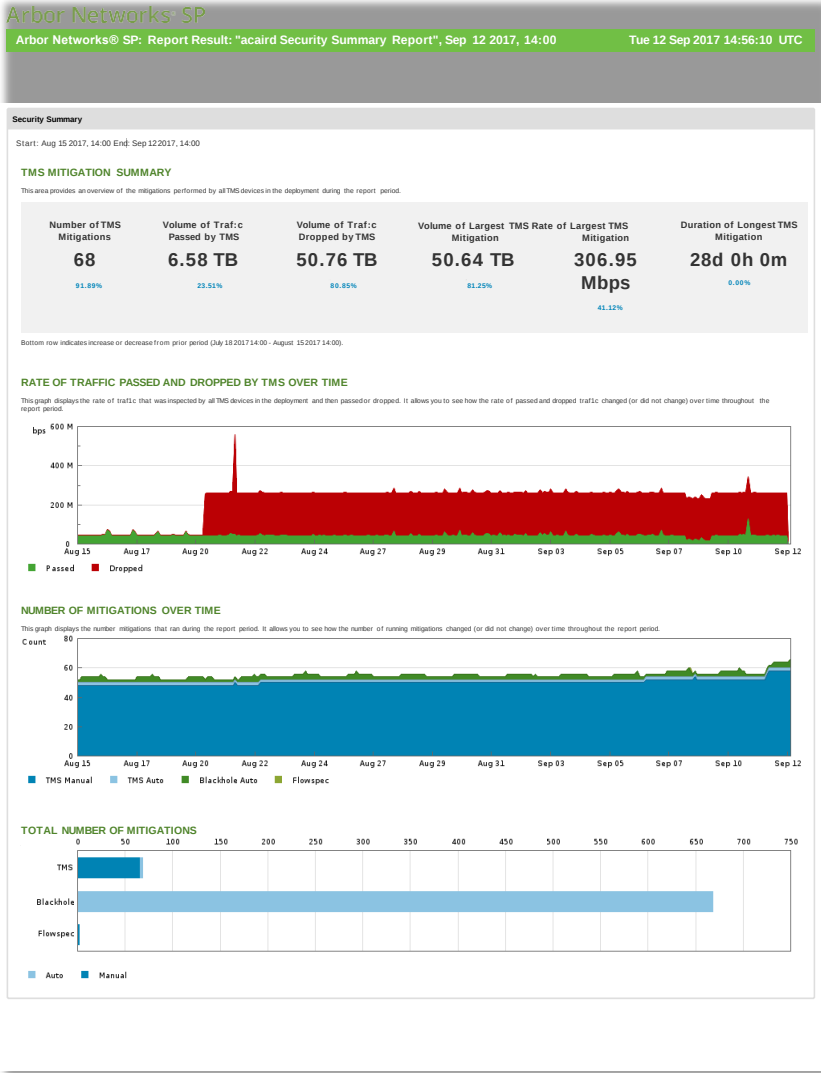
Защита авторитативных DNS серверов

SP/TMS 8.4

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



Executive reports



Atlas Global DDoS Report

Arbor Networks® SP



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

