

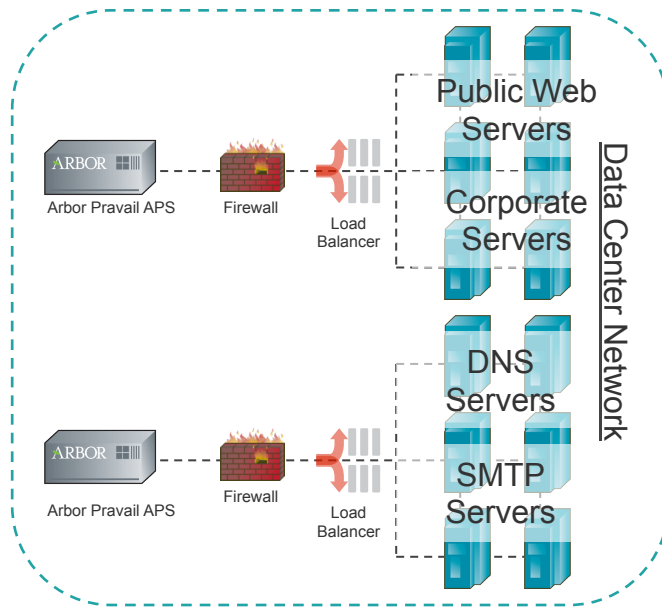


# Pravail 2.0 Technical Overview

Exclusive Networks

# Pravail Features and Benefits

**Arbor Pravail APS is the a CPE-based security appliance focused on stopping availability threats**



## ***'Out-of-the-Box' Protection***

- Immediate protection from threats with more control



## ***Advanced DDoS Blocking***

- Introduces new packet-based DDoS detection & mitigation



## ***Botnet Threat Mitigation***

- Block dynamic botnet-based DDoS attacks with AIF



## ***Simple Deployment Models***

- Easily fits IDC deployment including inline

CLOUD  
SIGNALING  
COALITION

## ***Cloud Signaling***

- Stop volumetric DDoS attacks by signaling upstream MSSPs

**ARBOR**  
NETWORKS

# ATLAS Intelligence Feed (AIF)

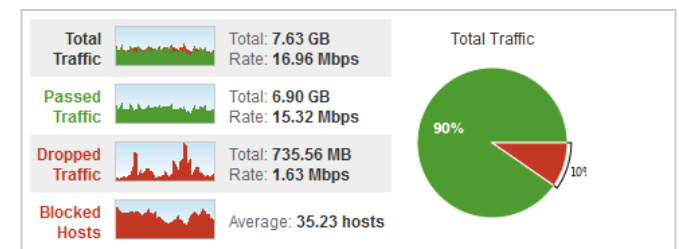


- Continuously updated feed of botnet threats to service availability
- Layer 7 fingerprints focused on inbound botnet attack traffic
  - Includes ASERT threat level and confidence assessment
- ASERT tracking **hundreds** individual botnets in the wild
  - More added nearly every day

**ARBOR SERT**  
Security Engineering & Response Team



Inbound HTTP Botnet Attacks  
ASERT Severity Levels  
IP Location Data

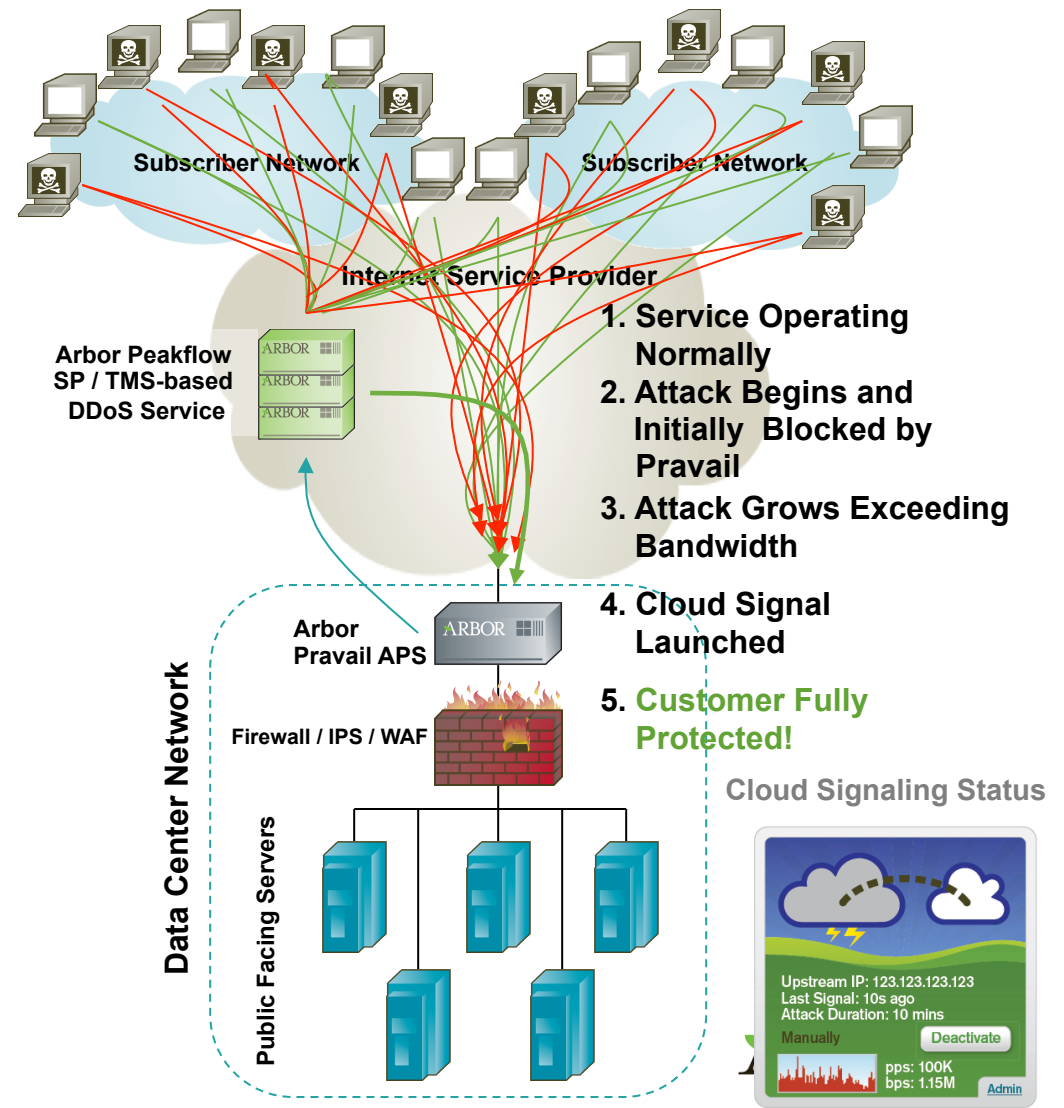


**ARBOR**  
NETWORKS

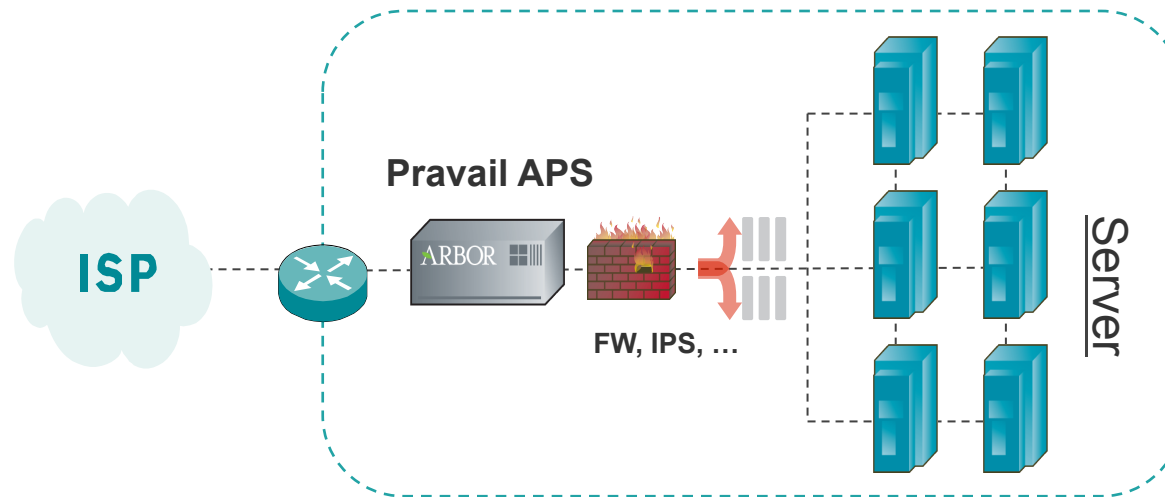
# Cloud Signaling

CLOUD  
SIGNALING  
COALITION

- Utilize *Cloud Signaling Coalition* members for **volumetric** protection
- Gain Volumetric & Application protection from a single console!



# Pravail 2.0 Availability Protection System



- **Availability** Protection System
- **Inline** layer-2 deployment (bump in the wire)
- **In front of** Firewall, IPS, WAF, load-balancer, etc ...
- Including **DPI** (layer 7) inspection of traffic
  - **AIF signatures** for detecting complex elements
- Detect and **protect** against attacks at **customer edge**



# The Failure of Existing Security Devices

Today's CPE-based security devices focus on integrity & confidentiality but not on availability

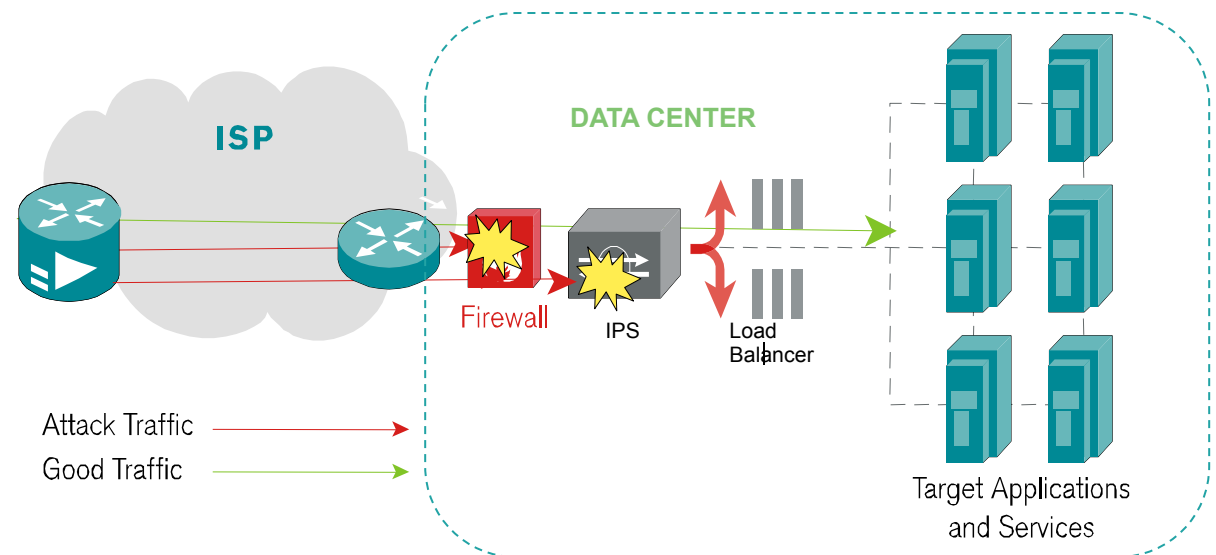


Information Security Triangle

Firewalls and IPS device do not solve the DDoS problem because they (1) are optimized for other security problems, (2) can't detect or stop distributed attacks, and (3) can not integrate with in-cloud security solutions.

IPS and firewall vendors will not win the arms race against hackers. **Stateful** device will always be threatened by state-exhausting attacks.

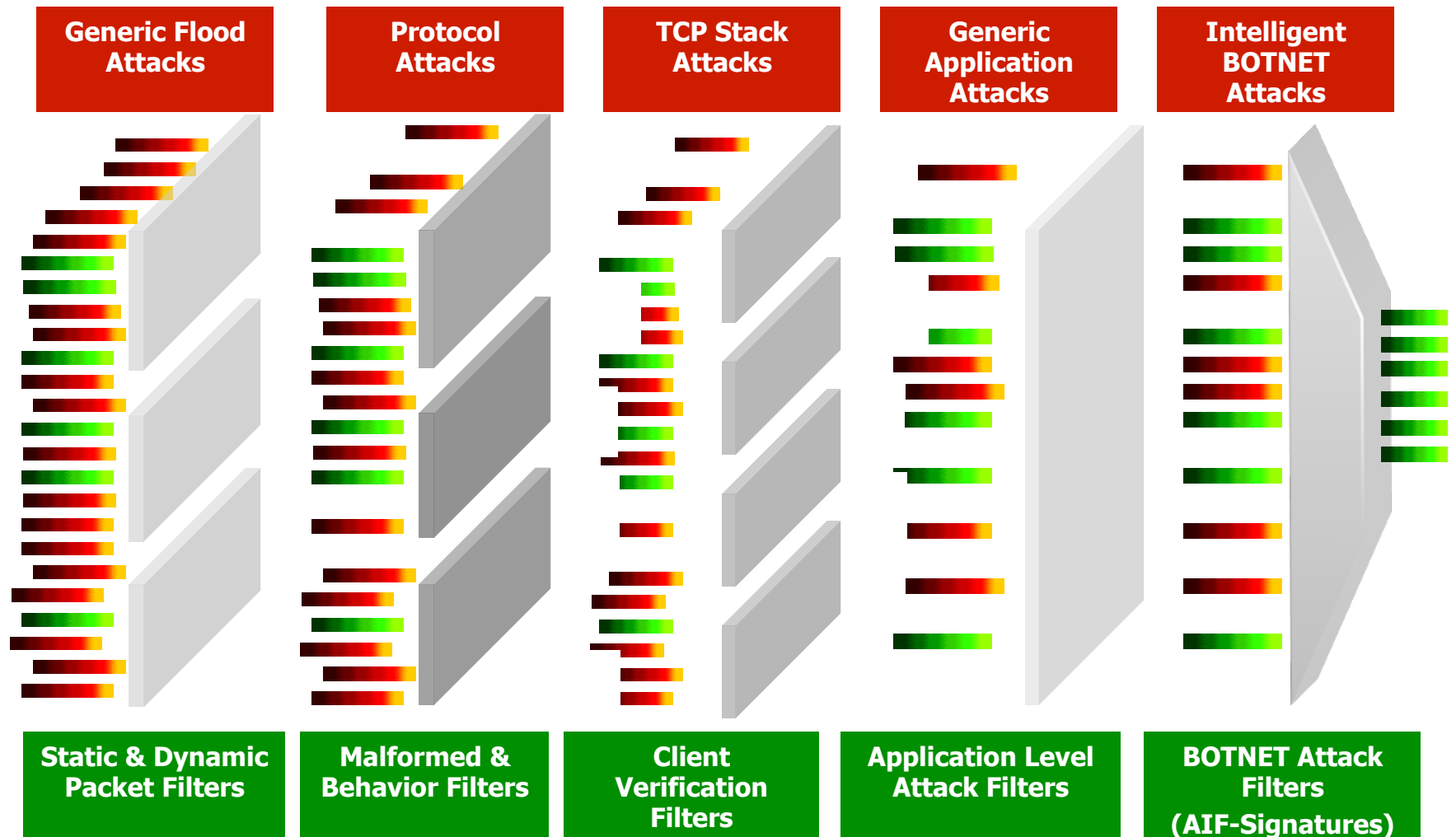
Product Family	Triangle	Benefit
Firewalls	Integrity / Confidentiality	Enforce network policy to prevent unauthorized access to data
Intrusion Prevention System	Integrity	Block break-in attempts causing data theft



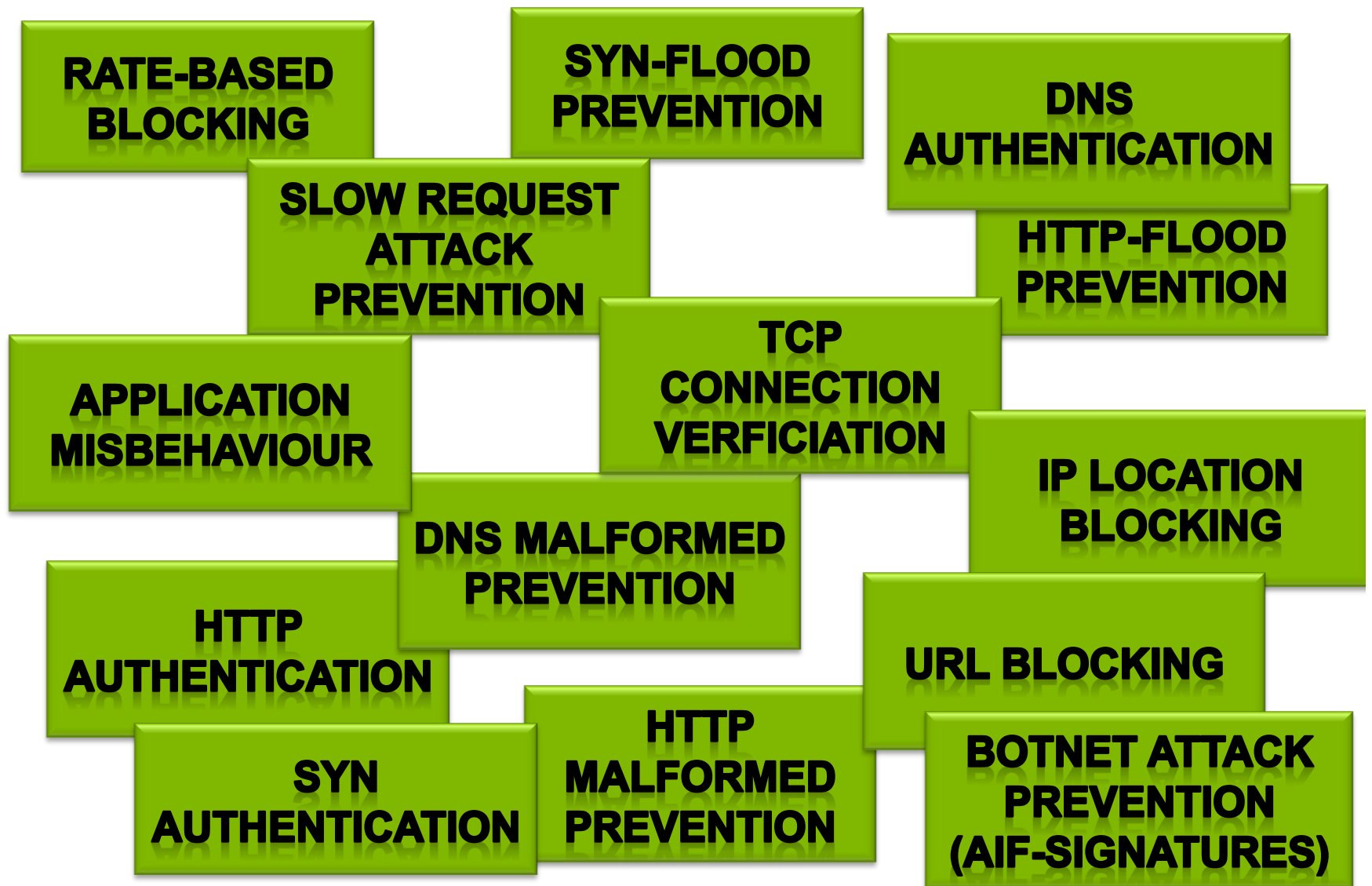
**Firewalls and IPS devices are part of the DDoS problem!**

# What happens to the traffic?

- Each client is checked by multiple intelligent filters



# Intelligent Filters ... some Examples





# Welcome to Pravail!

## Welcome to Arbor Networks' Pravail

Username:

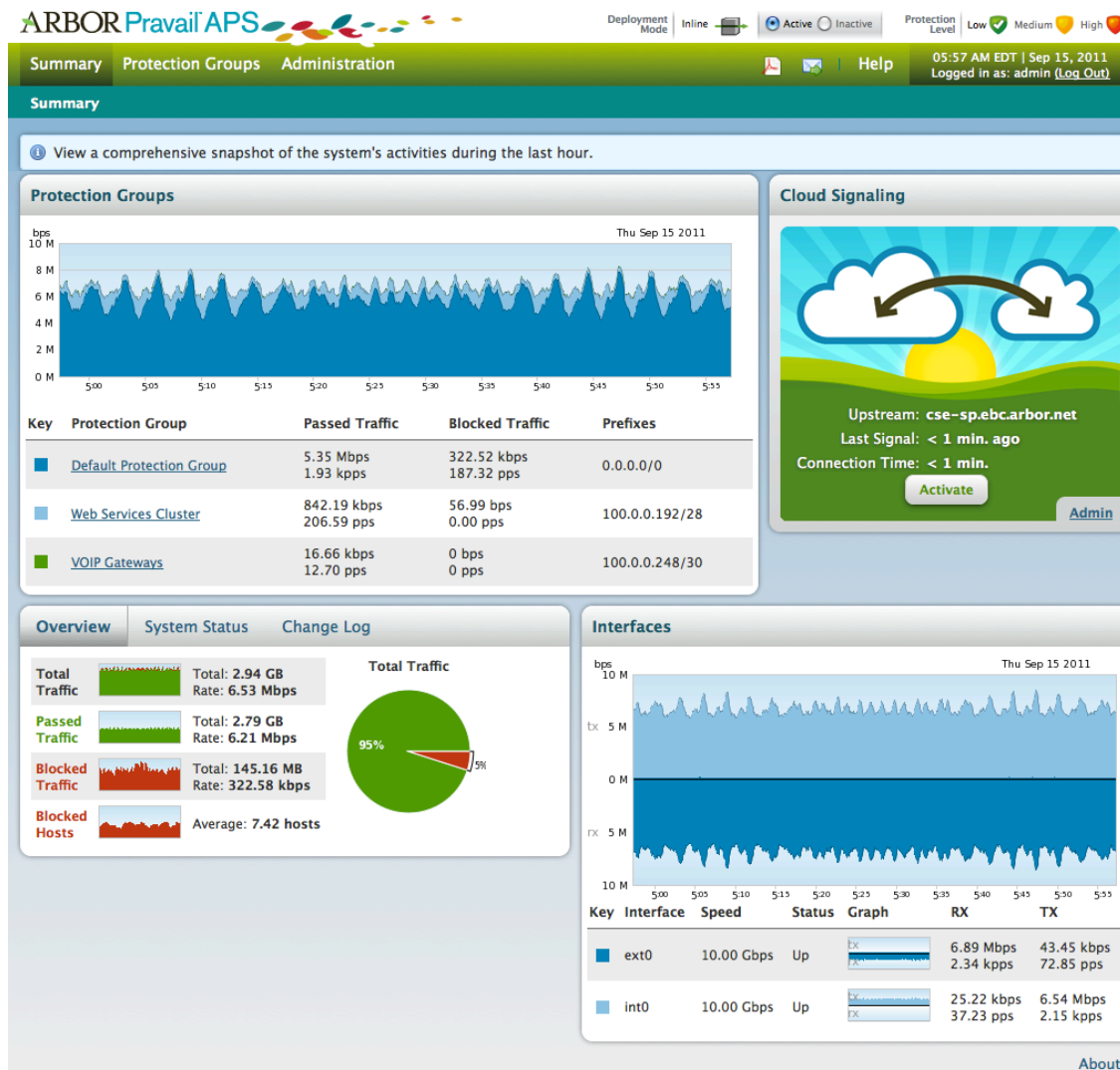
Password:

 Log In



**ARBOR**<sup>®</sup>  
NETWORKS

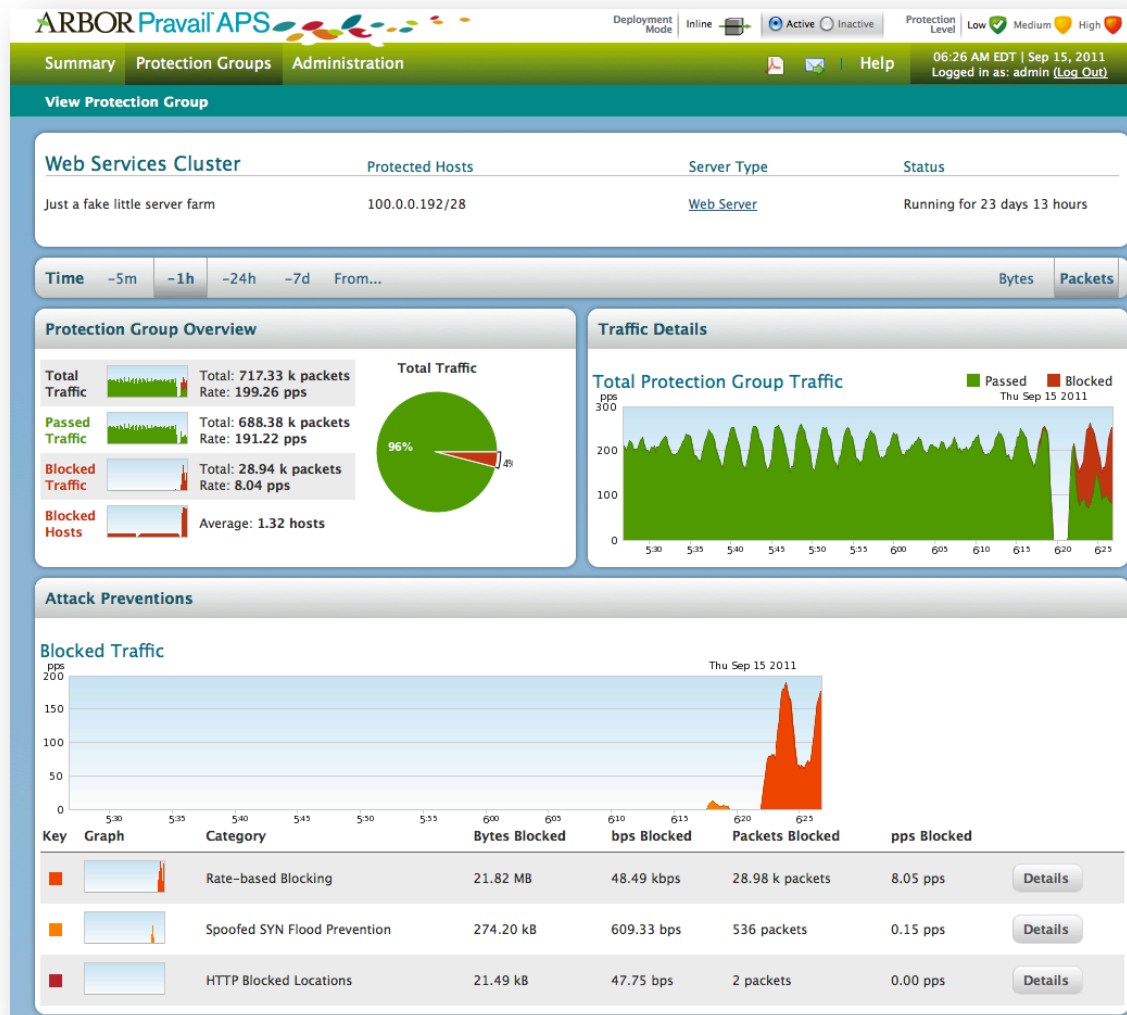
# Summary - Page



## ■ Overview:

- Protection Group(Group of Servers /Services)
- Interface Traffic
- Total Traffic
- Passed Traffic
- Blocked Traffic
- Protection Group
- Cloud Signaling Status
- System Status
- Change Log

# Protection Group – WebServer example - I



- A Protection Group is a individual set of IPs of the same Server/Service Type. E.g. WebServer

- Details:
  - Total Traffic
  - Passed Traffic
  - Blocked Traffic
  - Blocked Hosts
  - Details per Attack Prevention Type

- Options:
  - Time Period
  - BPS/PPS
  - PDF / EMAIL

**ARBOR**  
NETWORKS

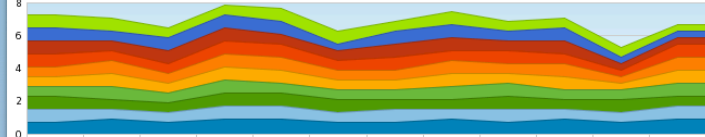
# Protection Group – II

## Web Traffic By URL

### Top URLs

requests per minute

Thu Sep 15 2011



Key Graph URL Requests Percent Request bps

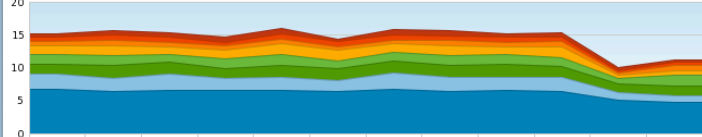
	livechat.iestorechat.com/...	42	4.88%	36.96 bps	
	livechat.iestorechat.com/...	42	4.88%	36.96 bps	
	livechat.iestorechat.com/...	42	4.88%	36.96 bps	

## Web Traffic By Domain

### Top Domains

requests per minute

Thu Sep 15 2011



Key Graph Domain Name Requests Percent Request bps

	iestorechat.com	365	42.44%	321.20 bps	
	tynt.com	115	13.37%	115.32 bps	
	collective-media.net	102	11.86%	170.14 bps	
	twitter.com	82	9.53%	156.26 bps	
	symantecliveupdate.com	77	8.95%	38.18 bps	
	photoworks.com	41	4.77%	19.95 bps	
	wxbug.com	39	4.53%	22.10 bps	
	vindicosuite.com	39	4.53%	119.60 bps	

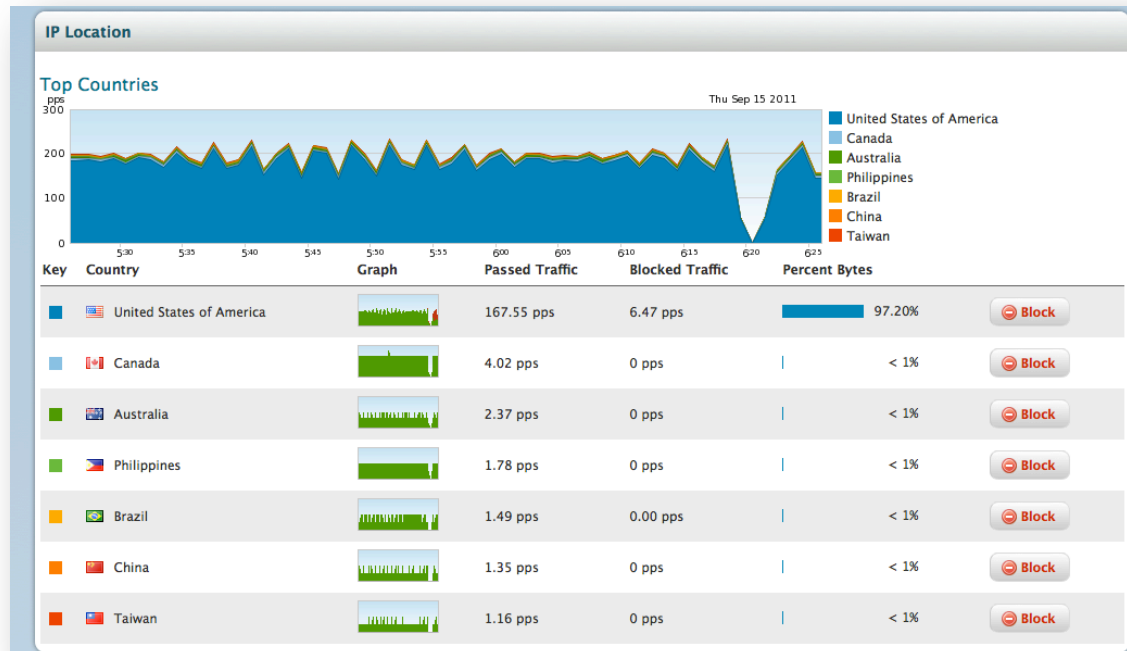
- URL statistics

- Domain statistics

- Option to easily BLOCK Domains / URLs

ARBOR<sup>®</sup>  
NETWORKS

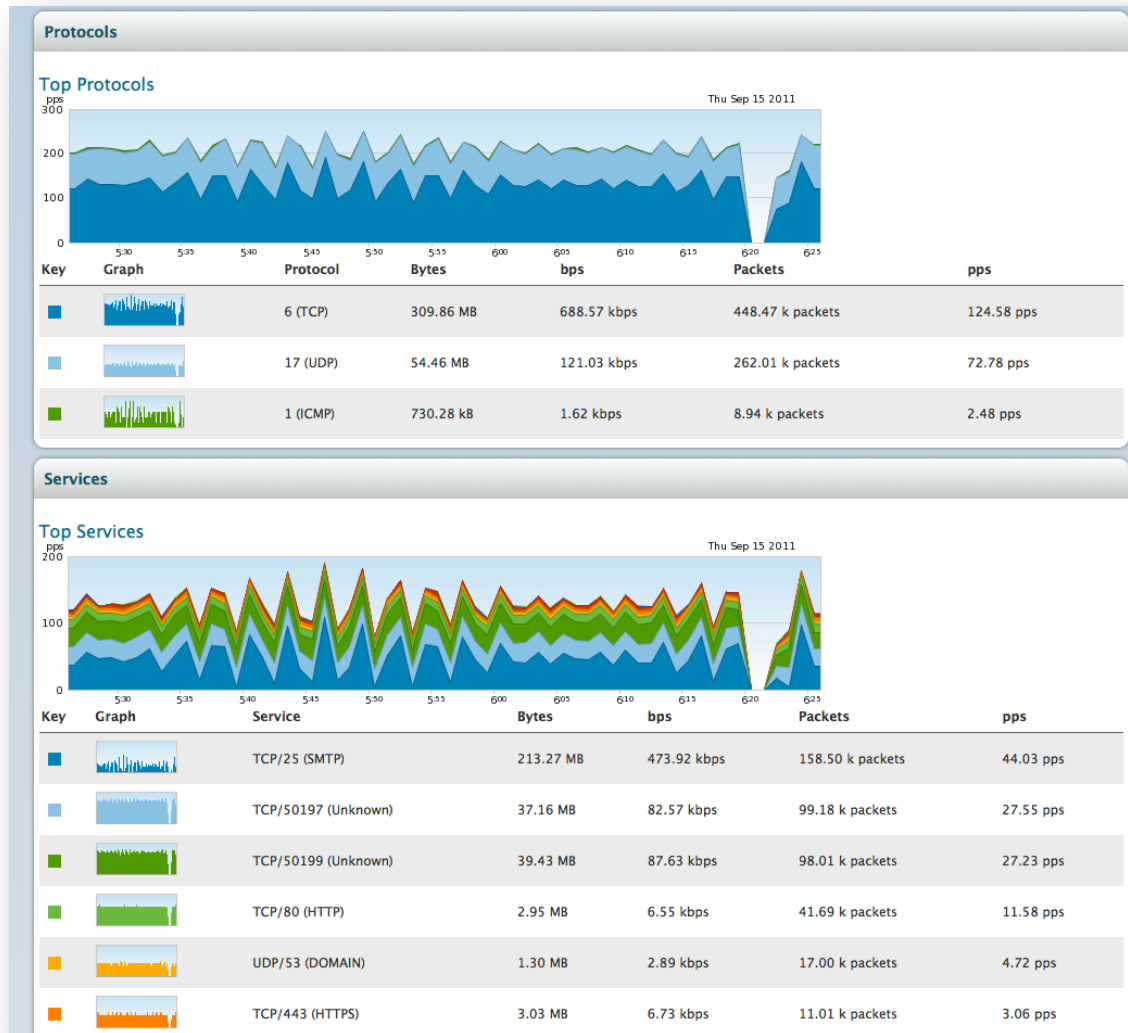
# Protection Group – III



- IP Location statistics
- Option to easily **BLOCK** attacking countries



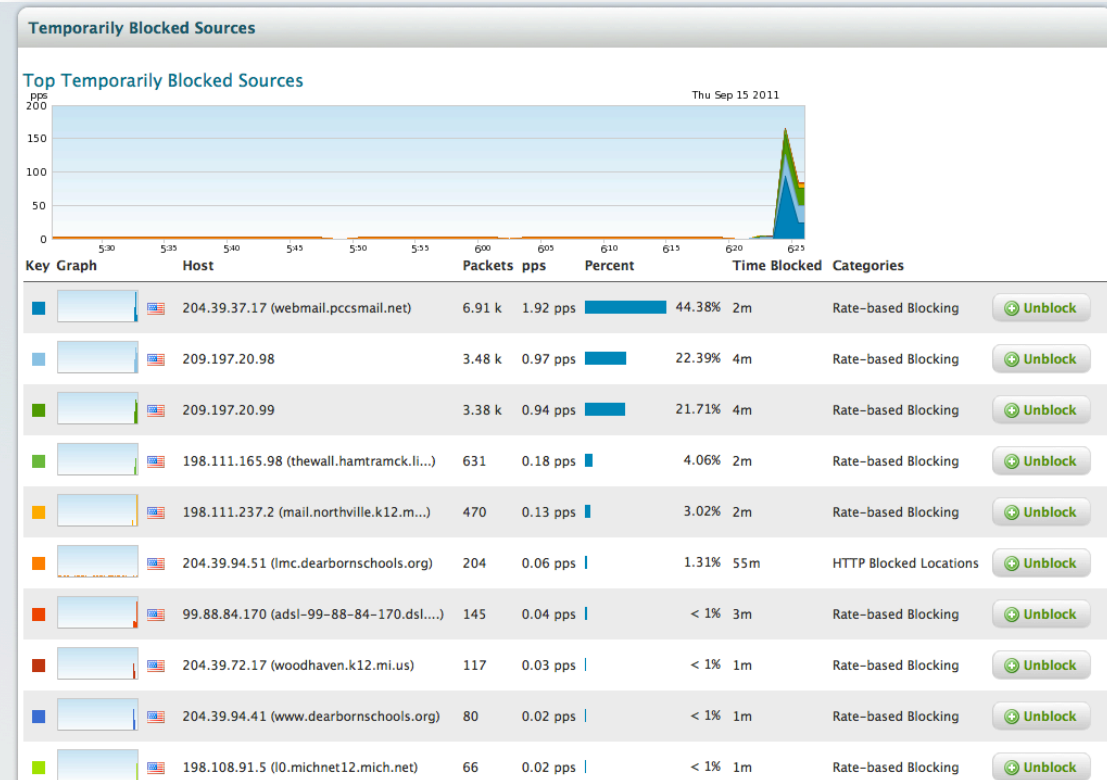
# Protection Group – IV



- Protocol statistics

- Service statistics

# Protection Group –V



- Blocked Hosts statistics
- Option to unblock hosts

# Summary – Mode, Protection Level, Cloud Help

**ARBOR Pravail APS**

Deployment Mode: ☒ Active ☐ Inactive

Protection Level: ☒ Low ☐ Medium ☐ High

Cloud Signaling: ☒ Status ☐ Automatic ☐ Manually

Summary

View a comprehensive snapshot of the system's activities during the last hour.

Cluster	842.19 kbps	56.99 bps	100.0.0.192/28
Web Services Cluster	206.59 pps	0.00 pps	
VOIP Gateways	16.66 kbps	0 bps	
	12.70 pps	0 pps	

Overview System Status Change Log

Total Traffic: 2.94 GB, Rate: 6.53 Mbps

Passed Traffic: 2.79 GB, Rate: 6.21 Mbps

Blocked Traffic: 145.16 MB, Rate: 322.58 kbps

Blocked Hosts: Average: 7.42 hosts

Cloud Signaling: Upstream: cse-sp.ebc.arbor.net, Last Signal: < 1 min. ago, Connection Time: < 1 min. [Activate]

- **Mode:**
  - Active
  - Inactive
- **Protection Level:**
  - Low
  - Medium
  - High
- **Cloud Signaling**
  - Status
  - Automatic
  - Manually

# Prevention Types – Details I/VI

Generic Server

Web Server

DNS Server

VOIP Server

Blacklist

Whitelist

Filter List

Uses configurable filters to drop or pass traffic. Create drop rules to drop the traffic that matches the specified FCAP expression. Create pass rules to pass the matching traffic without involving further countermeasures.

Filter FCAP Expressions

# Localhost  
drop net 127.0.0.0/8  
# Current network (RFC 1700)  
#drop net 0.0.0.0/8

# Localhost  
drop net 127.0.0.0/8  
# Current network (RFC 1700)  
#drop net 0.0.0.0/8

# Localhost  
drop net 127.0.0.0/8  
# Current network (RFC 1700)  
#drop net 0.0.0.0/8

Rate-based Blocking

Detects sources that exceed the configured thresholds, and then places those sources on the temporary blocked hosts list.

Bits per Second Threshold

bps

bps

bps

Packets per Second Threshold

pps

10000

pps

5000

pps

Payload Regular Expression

Matches packets to the configured TCP or UDP ports and a regular expression, and then drops or passes the packets depending on the setting below.

Payload Regular Expression TCP Ports

Payload Regular Expression UDP Ports

Payload Regular Expression

# Prevention Types – Details II/VI

## Spoofed SYN Flood Prevention

Initiates a three-way handshake with the hosts that initiate TCP connections and drops the traffic from hosts that do not respond properly.

Enable Spoofed SYN Flood Prevention

Enabled

Disabled

Enabled

Disabled

Enabled

Disabled

HTTP Authentication Ports

80, 8080

80, 8080

80, 8080

HTTP Redirect Authentication

Enabled

Disabled

Enabled

Disabled

Enabled

Disabled

HTTP Soft Reset Authentication

Enabled

Disabled

Enabled

Disabled

Enabled

Disabled

TCP Out of Sequence Authentication

Enabled

Disabled

Enabled

Disabled

Enabled

Disabled

Ignore Destination Ports

## TCP Connection Reset

Blocks TCP connections that fail to make significant progress thereby protecting the server against slow request attacks. Sources that have multiple consecutive connections blocked will be placed on the temporary blocked sources list.

Enable TCP Connection Reset

Enabled

Disabled

Enabled

Disabled

Enabled

Disabled

Minimum Request Bit Rate

bps

200 bps

1000 bps

TCP Connection Initial Timeout

10 seconds

10 seconds

5 seconds

Initial Timeout Required Data

1 bytes

20 bytes

50 bytes

Consecutive Violations before Blocking Source

5

3

3

ARBOR  
NETWORKS



# Prevention Types – Details III/VI


## DNS Authentication

Authenticates DNS requests and drops those that cannot be authenticated within a specified time.

		
<input type="button" value="Enabled"/> <input checked="" type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input checked="" type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input checked="" type="button" value="Disabled"/>

## Block Malformed DNS Traffic

Drops the DNS requests on port 53 that do not conform to RFC standards.

		
<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input checked="" type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input checked="" type="button" value="Disabled"/>

## DNS Rate Limiting

Drops the DNS request traffic that exceeds the configured rate limit, and then blacklists the source host.

		
DNS Query Rate Limit <input type="text"/> queries/s	<input type="text"/> queries/s	<input type="text"/> queries/s




## DNS NXDomain Rate Limiting

Drops the traffic from any host that generates more consecutive failed DNS requests than the configured limit, and then blacklists the source host.

		
DNS NXDomain Rate Limit <input type="text" value="100"/> failed queries/s	<input type="text" value="50"/> failed queries/s	<input type="text" value="25"/> failed queries/s

## DNS Regular Expression

Drops the traffic for established TCP connections that remains idle for longer than the configured limits, and then blacklists the source hosts.

		
DNS Regular Expressions		
1. <input type="text"/>	1. <input type="text"/>	1. <input type="text"/>
2. <input type="text"/>	2. <input type="text"/>	2. <input type="text"/>
3. <input type="text"/>	3. <input type="text"/>	3. <input type="text"/>
4. <input type="text"/>	4. <input type="text"/>	4. <input type="text"/>
5. <input type="text"/>	5. <input type="text"/>	5. <input type="text"/>

# Prevention Types – Details IV/VI

## Malformed HTTP Filtering

Drops the HTTP traffic that does not conform to RFC standards for request headers, and then blacklists the source hosts.

Enabled

Disabled

Enabled

Disabled

Enabled

Disabled

## HTTP Rate Limiting

Drops the HTTP request traffic that exceeds any of the configured rate limits.

HTTP Request Limit

reqs/s

500

reqs/s

100

reqs/s

HTTP URL Limit

URLs/s

10

URLs/s

15

URLs/s

## HTTP Header Regular Expressions

Blocks HTTP requests which match a configured regular expression.

Header Regular Expressions

1.
2.
3.
4.
5.

1.
2.
3.
4.
5.

1.
2.
3.
4.
5.

# Prevention Types – Details V/VI

## Traffic Shaping

Analyzes the traffic that was not dropped by any of the other countermeasures. Any traffic that matches the specified FCAP expression and exceeds the configured rate limits is dropped.

Maximum bps  bps

Maximum pps  pps

Filter

proto icmp

bps

1500 pps

proto icmp

bps

1000 pps

proto icmp

## TCP SYN Flood Detection

Detects SYN floods above the configured rates.

Enable SYN Flood Detection

Enabled

Disabled

Syn Ack Delta Rate

50

Syn Rate

150

Enabled

Disabled

30

90

Enabled

Disabled

15

45

## ICMP Flood Detection

Detects ICMP floods above the configured rates.

Enable ICMP Flood Detection

Enabled

Disabled

ICMP Rate

50

Enabled

Disabled

20

Enabled

Disabled




5

NETWORKS

# Prevention Types – Details VI/VI




### Botnet Prevention

Blocks traffic that matches the signatures used by bots.

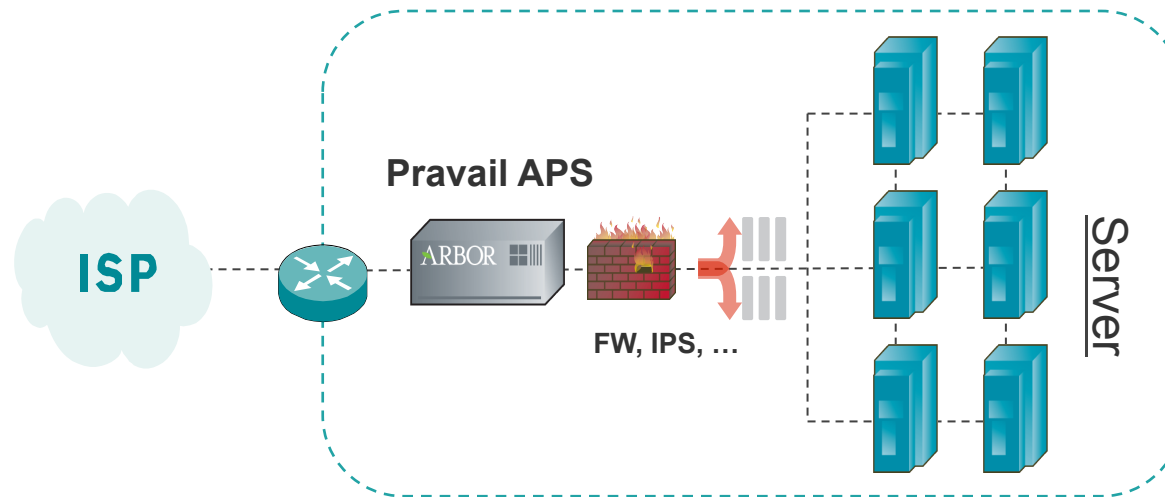
			
Enable Basic Botnet Prevention	<input type="button" value="Enabled"/> <input checked="" type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>
Enable AIF Botnet Signatures	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>
Prevent Slow Request Attacks	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>

### Application Misbehavior

Blocks traffic from sources that repeatedly interrupt HTTP requests, and places those sources on the temporary blocked sources list.

			
Interrupt Count	<input type="text" value="10"/>	<input type="text" value="5"/>	<input type="text" value="3"/>

# Pravail 2.0 APS - Cloud Signaling



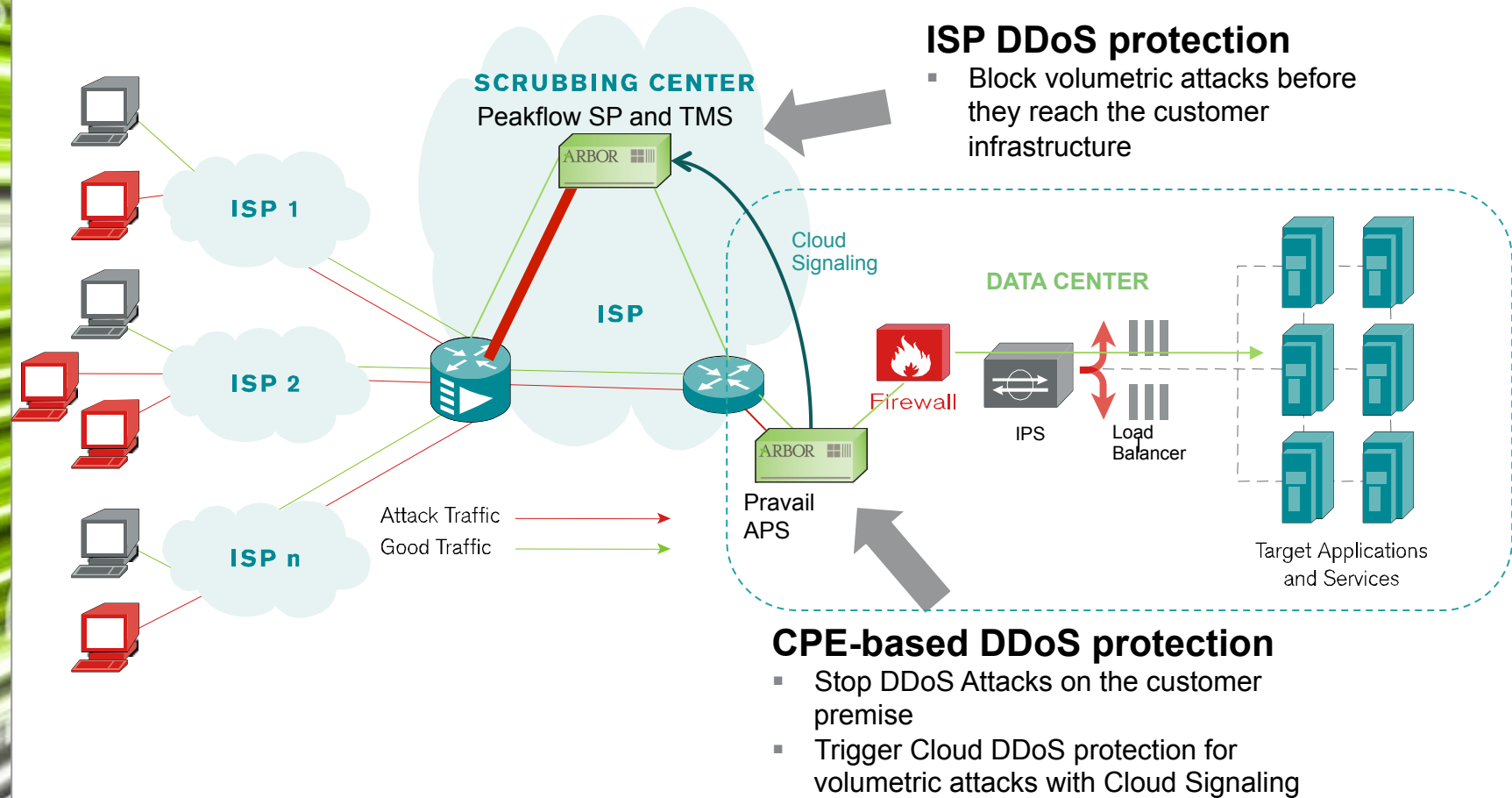
## Pravail stand-alone inline protection

- Detects and defends attacks at customer edge
- Can ask for help to protect from volumetric attacks larger than uplinks – mitigation must be performed upstream



# ISP - Cloud Signaling as a Managed Service

## ISP uses Peakflow SP and TMS products in the cloud



**ARBOR**  
NETWORKS



**Thank You**