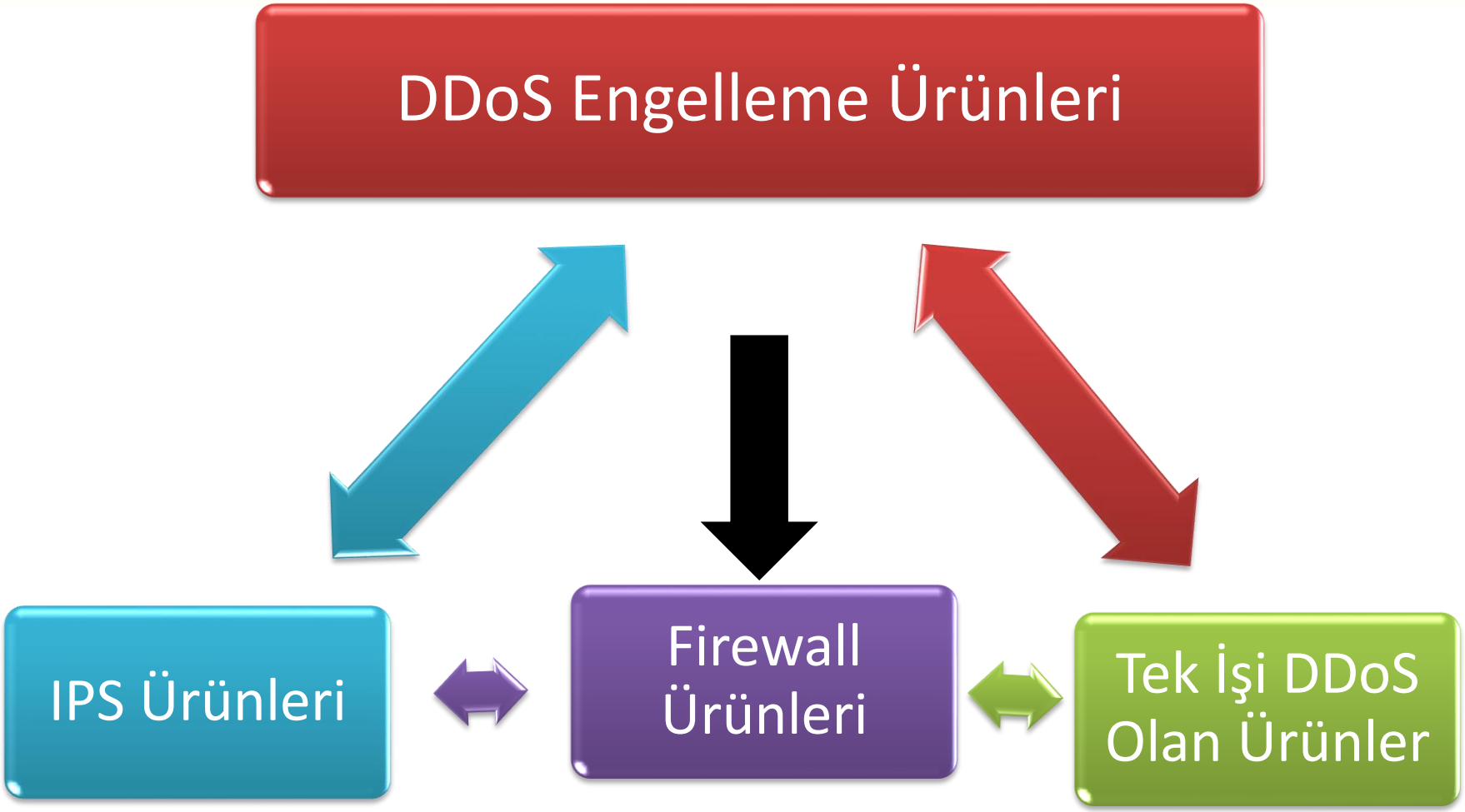
DDoS Engelleme Ürünleri

DDoS Engelleme



Engelleme Yöntemleri

- Genel engelleme yöntemleri
- SYN Flood için Syncookie/SynProxy
- UDP flood için rate limiting
- HTTP Get flood için rate limiting/session limiting
- ACK flood için scrubbing
- FIN flood için scrubbing
- ICMP flood için firewall özellikleri

Günümüz “Enterprise Security” Ürünleri

- Saldırganın silahlarını ve gücünü gördük, buna karşılık güvenlik dünyasının ürettiği savunma sistemlerinin özelliklerine ve güçlerine bakalım
- Firewall/IPS sistemleri DDOS saldırılarına nr kadar dayanıklı….
  - Gelebilecek itirazlar: Firewall/IPS sistemleri DDOS engelleme amaçlı değildir(!)

Fortinet Firewall Limitleri

Technical Specifications





HARDWARE SPECIFICATIONS	FortiGate-1000A	FortiGate-1000AFA2	FortiGate-3016B	FortiGate-3600A	FortiGate-3810A
10/100/1000 Interfaces (Copper)	10	10	8	8	8
1Gb SFP Interfaces	0	2	2	2	2 - 26*
SFP Transceivers Provided	NA	2	2	2	2 (SX)
USB Ports	1	1	1	1	1
AMC Expansion Slots	0	0	0	width	2 single width 2 double width
SYSTEM PERFORMANCE					
Concurrent Sessions	1,100,000	1	0	0	2,000,000
New Sessions/Second	15,000	1	1	1	40,000
Firewall Throughput (Gbps)	2 Gbps	2 Gbps	16 - 20* Gbps	6 - 10* Gbps	7 - 37* Gbps
VPN Throughput (IPSec)	600 Mbps	600 Mbps	12 - 15* Gbps	0.8 - 3.8* Gbps	1 - 19* Gbps
IPS Throughput	1 Gbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps
Antivirus Throughput	200 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps
Unlimited Concurrent Users	Yes	Yes	Yes	Yes	Yes
Site-to-site IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000
Client-to-Site IPSec VPN Tunnels	10,000	10,000	64,000	64,000	64,000
Number of Concurrent SSL Users (Recommended)	1,000	1,000	2,000	3,000	5,000
Policies	100,000	100,000	100,000	100,000	100,000
Virtual Domains (VDOMS) (standard / with optional license)	10 / NA	10 / NA	10 / 250	10 / 250	10 / 250

20Mb hat=40.000 pps
(20x1024x1024/8/60)
50 saniyede 2.000.000 session

Netscreen Firewall Limitleri

NETSCREEN-5200

NETSCREEN-5400

Specifications

	NETSCREEN-5200	NETSCREEN-5400
Maximum Performance and Capacity[1]		
ScreenOS® version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (large packets)[2]	10/8 Gbps	30/24 Gbps
Firewall performance (small packets)	4 Gbps	12 Gbps
Firewall Packets Per Second (64 byte)	6 M PPS	18 M PPS
AES256+SHA-1 VPN performance[2]	5/4 Gbps	15/12 Gbps
3DES+SHA-1 VPN performance[2]	5/4 Gbps	15/12 Gbps
Maximum concurrent sessions[3]	1,000,000	2,000,000[(9)]
New sessions/second[10]	26,500/22,000	26,500/22,000

Netscreen ISG Limitleri

ISG 2000

	ISG1000	ISG2000
Maximum Performance and Capacity[1]		
ScreenOS® version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (large packets)	2 Gbps	4 Gbps
Firewall performance (small packets)	1 Gbps	2 Gbps
Firewall packets per second (64 byte)	1.5 M PPS	3 M PPS
AES256+SHA-1 VPN performance	1 Gbps	2 Gbps
3DES+SHA-1 VPN performance	1 Gbps	2 Gbps
Maximum concurrent sessions[3]	500,000	1,000,000
New sessions/second	20,000	23,000
Maximum security policies	10,000	30,000

Checkpoint Power-1 Limitleri

Check Point Power-1 Appliances

Security for high-performance environments

Power-1 11000 series

Power-1 5075

Power-1 9075

Hardware Specifications

Hardware Specifications

Appliance	Power-1 5075	Power-1 9075	Power-1 11000 Series		
			11065	11075	11085
Software Edition	R65, R70	R65, R70	R70	R70	R70
Operating System	Secure Platform	Secure Platform	Secure Platform	Secure Platform	Secure Platform
10/100/1000 Ports	10/14	14/18	14/18	14/18	14/18
10Gb ports	2 optional	4 optional	4 optional	4 optional	4 optional
Firewall Throughput[1]	9 Gbps	16 Gbps	15 Gbps	20 Gbps	25 Gbps
VPN Throughput[1]	2.4 Gbps	3.7 Gbps	3.7 Gbps	4 Gbps	4.5 Gbps
Concurrent Sessions	1.2 Million	1.2 Million	1.2 Million	1.2 Million	1.2 Million

TippingPoint 10Gb IPS Limitleri

data_sheet

TippingPoint_N-Platform

Technical Specifications

Hardware	TippingPoint 660N	TippingPoint 1400N	TippingPoint 2500N		TippingPoint 5100N	
Performance						
Inspected Throughput [1]	750 Mbps	1.5 Gbps	3 Gbps		5 Gbps	
Network Throughput [2]	750 Mbps	1.5 Gbps	15 Gbps		15 Gbps	
Typical Latency [3]	< 80 microseconds	< 80 microseconds	< 80 microseconds		< 80 microseconds	
Concurrent Network Sessions [4]	6,500,000	6,500,000	10,000,000 [5]		10,000,000 [5]	
Security Contexts [6]	1,200,000	1,200,000	2,600,000		2,600,000	
Connections Per Second	115,000	115,000	230,000		230,000	
Scalability						
Interfaces	1 GbE	1 GbE	10 GbE	1 GbE	10 GbE	1 GbE
Ethernet Ports	(20) 10/100/1000	(20) 10/100/1000	(2) 10 GbE XFP	(20) 10/100/1000	(2) 10 GbE XFP	(20) 10/100/1000
Port Quantity/Type	(10) Copper/(10) SFP	(10) Copper/(10) SFP	(2) 10 GbE XFP	(10) Copper/(10) SFP	(2) 10 GbE XFP	(10) Copper/(10) SFP
Number of Port Segments	10	10	1	1	1	1
Zero Power HA	External	External	Modular	External	Modular	External

Güvenlik Duvarları ve DDoS Saldırıları

- Güvenlik duvarları DDoS saldırıları engelleme amaçlı düşünülmemiştir
  - İstisnalar mevcuttur, Packet Filter gibi
- Genellikle izin ver, engelle, session tut gibi özelliklere sahiptir
  - Bazı firewallar syn cookie, syn proxy, rate limiting özelliklerine sahiptir
- Session tabloları sınırlıdır
  - Max değer 10.000.000
- Donanım tabanlı olmayanlar ciddi saldırılar karşısında işe yaramaz

Linux Iptables

- Linux işletim sistemi syncookie özelliğine sahiptir
  - Fakat bu özellik sadece işletim sisteminin kendini korumak içindir
  - Linux iptables tarafından korunan sistemlere doğru syncookie özelliği yoktur
- Rate limiting özelliği vardır fakat tasarım hatasına sahiptir!

```
iptables -I INPUT -p tcp --dport 25 -i eth0 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 -j DROP
```

- Ciddi saldırılar karşısında yetersizdir!

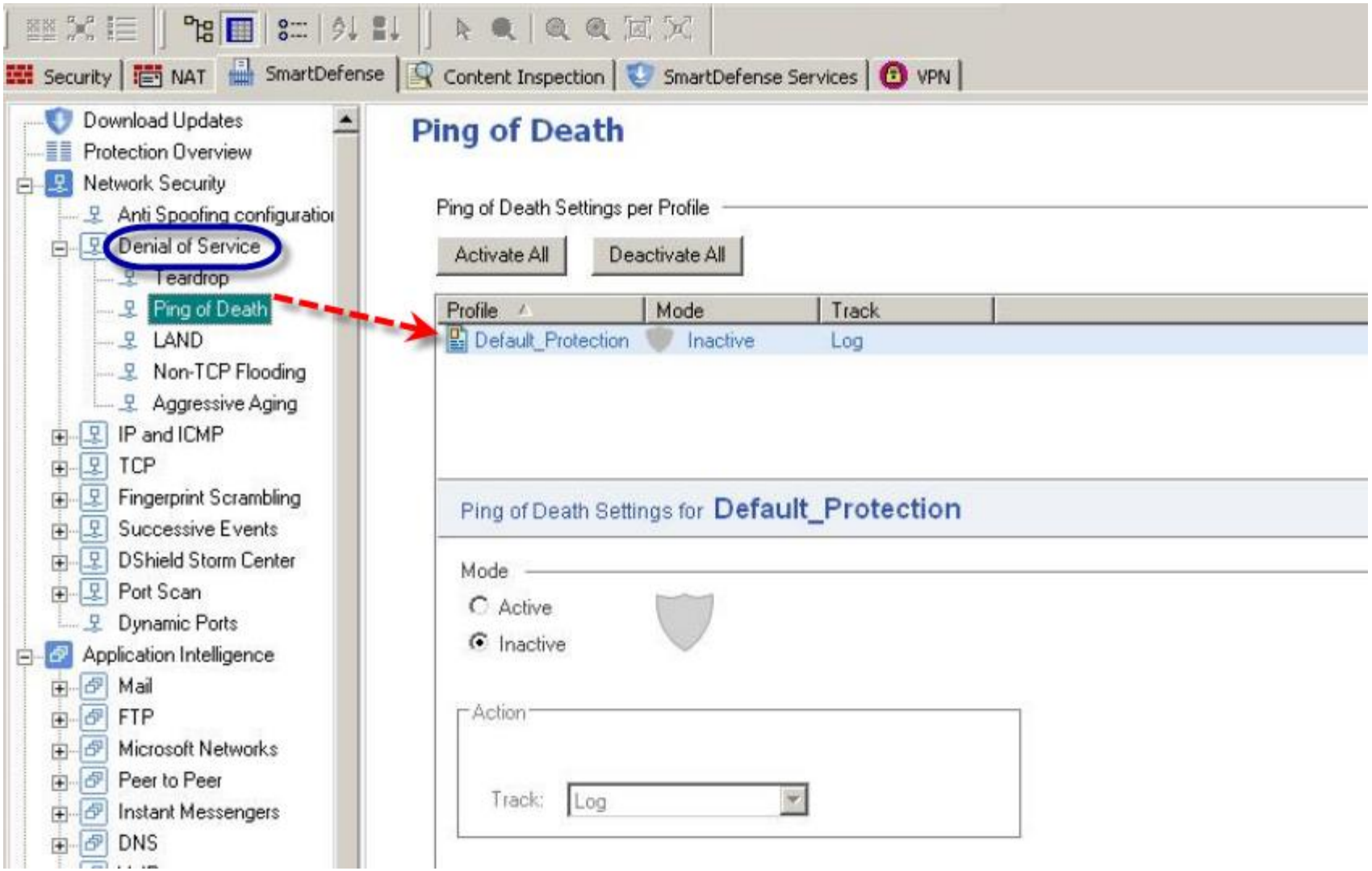
OpenBSD Packet Filter

- DDoS engelleme amaçlı geliştirilmiş güvenlik duvarı
- Her tür engelleme özelliği bulunmaktadır
  - Syn proxy
  - Rate limiting
  - IP başına session limit, zaman limiti
  - Sahte ip geçirmeme özelliği
  - FIN,ACK,NULL Flood özellikleri
  - Adaptive timeout özelliği
  - ...
- 1 Gb'e kadar DDoS saldırılarında rahatlıkla kullanılabilir

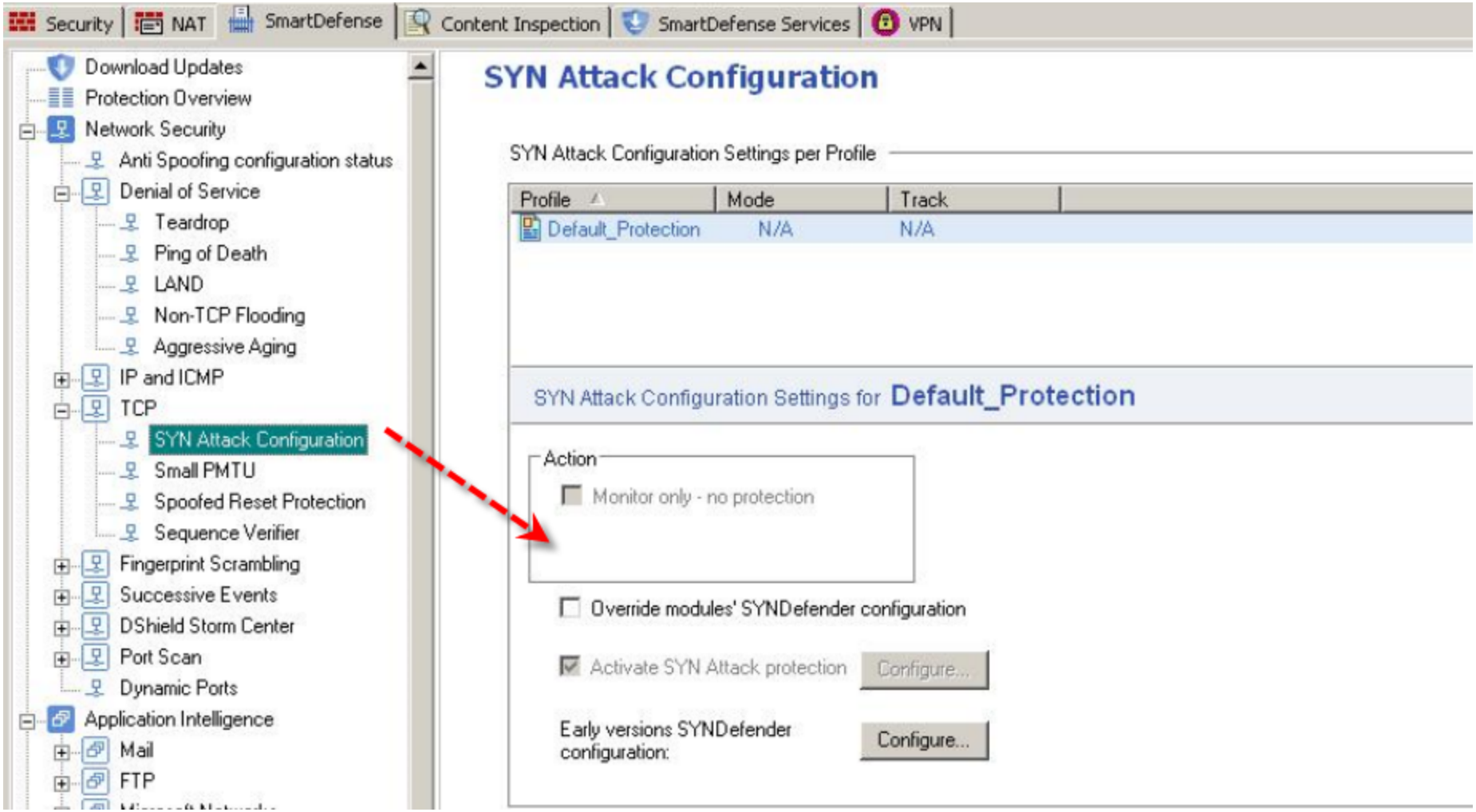
CheckPoint

- En fazla tercih edilen Güvenlik duvarı yazılımı
- Donanım versiyonları da vardır fakat Intel tabanlıdır
  - İstisnalar mevcut olabilir
- Eski tip DoS/DDoS saldırılarına karşı Smartdefense eklentisi kullanılabilir
- Yeni tip DDoS saldırılarına karşı dayanıksızdır!
- Rate limiting özelliği vardır
  - IP başına zamana bağlı paket geçirme

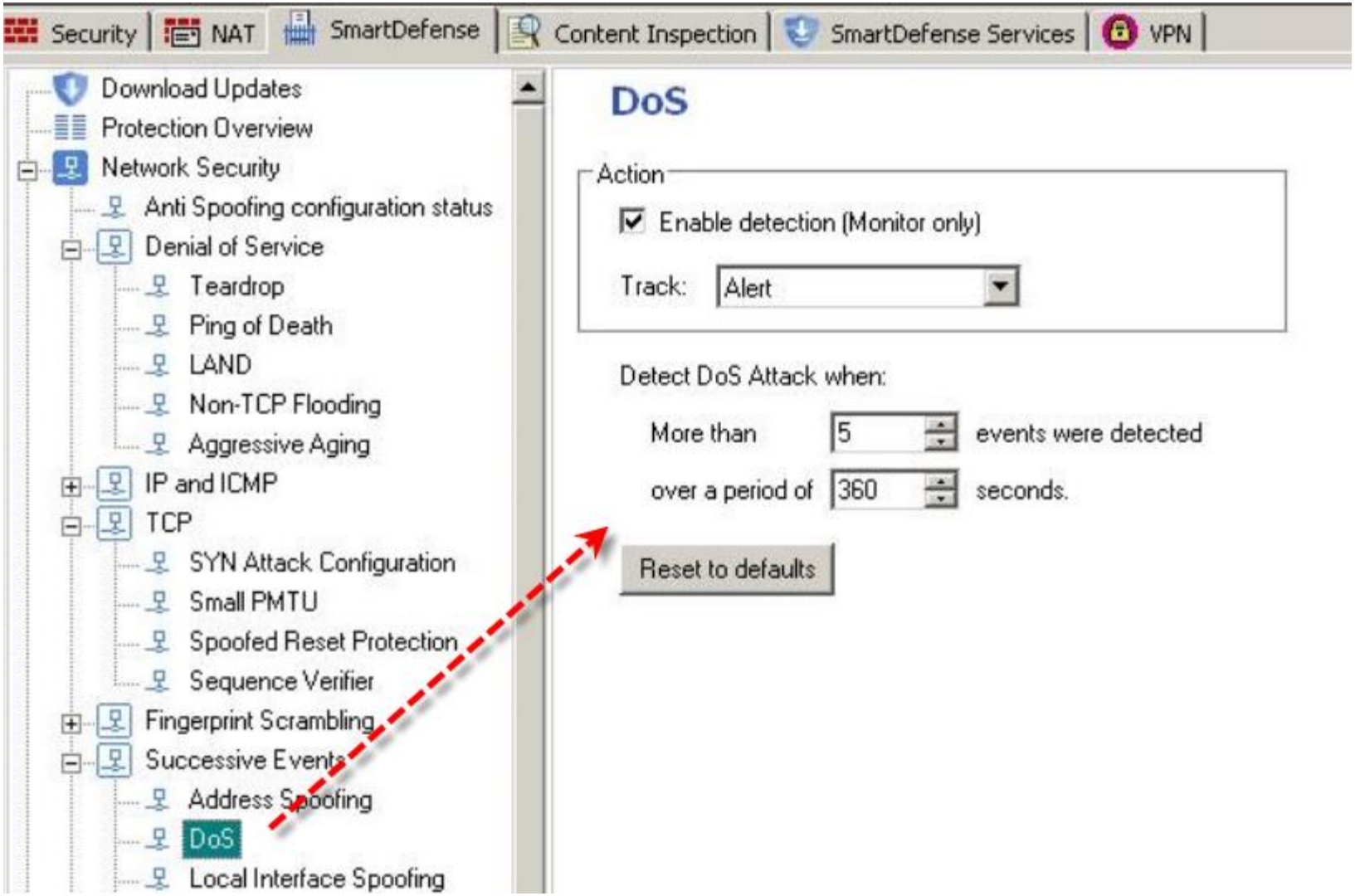
Ping Of Death Koruması



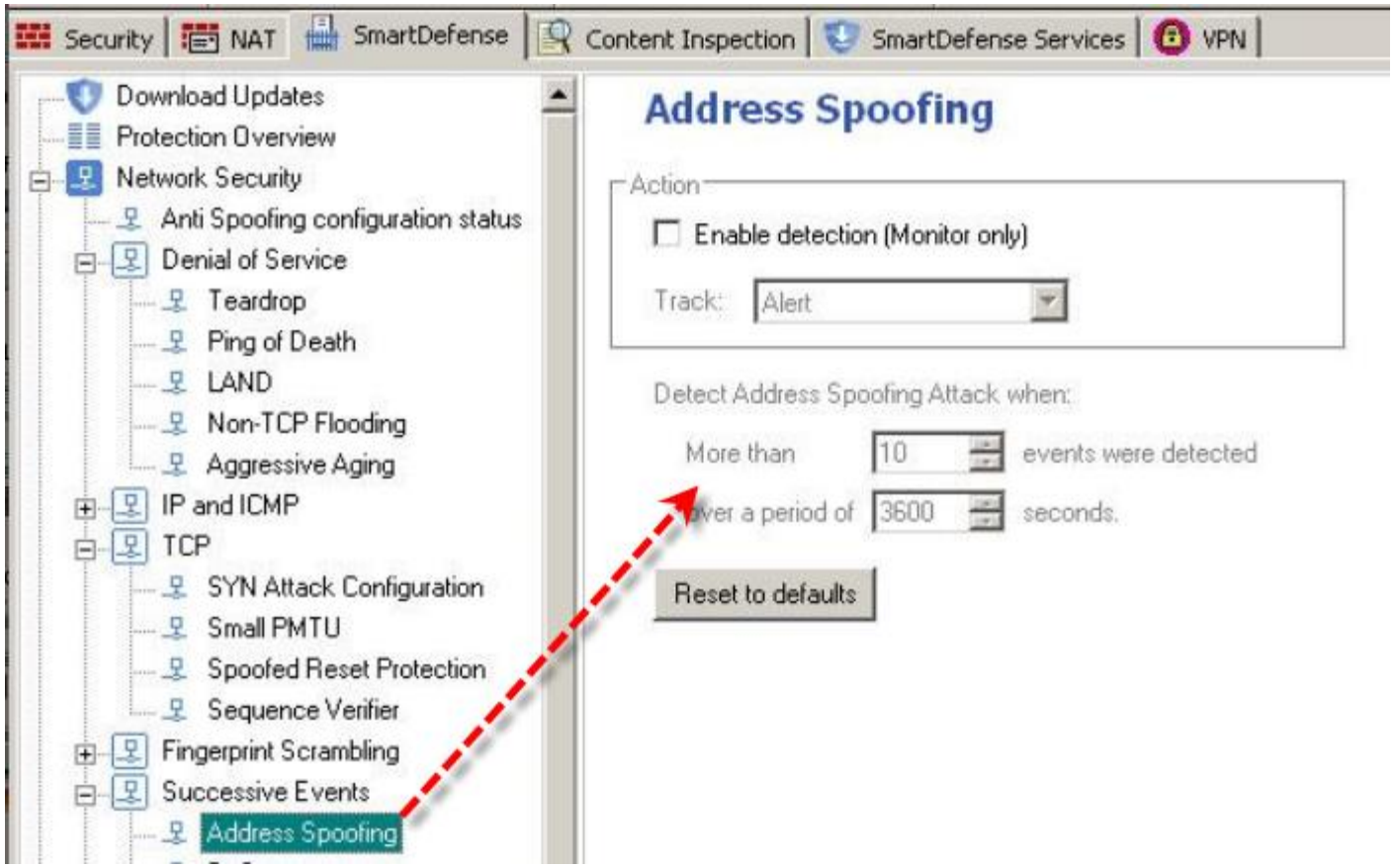
Syn Flood Koruması



Rate Limiting Özelliği



Sahte IP Engelleme Koruması



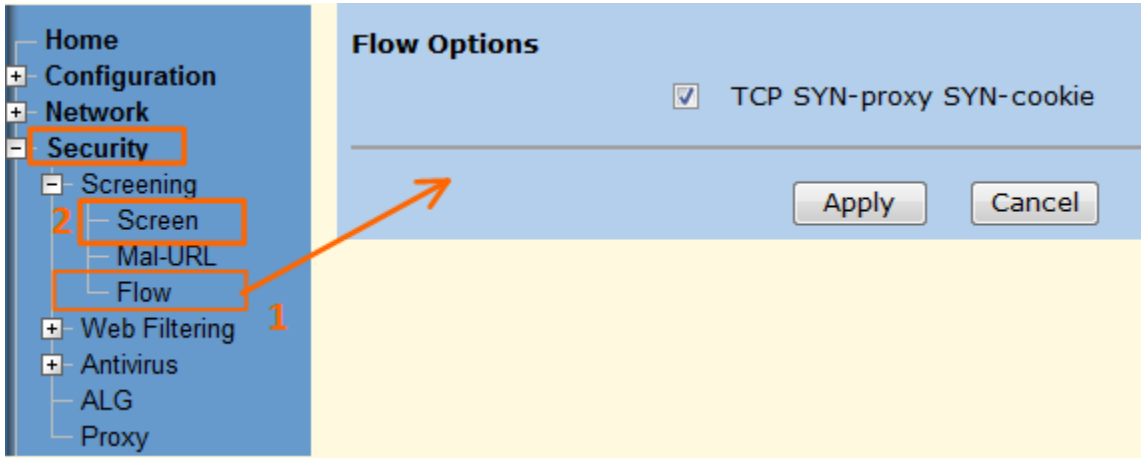
Netscreen

- Donanım tabanlı güçlü sistemlerdir
- Eski tip ve yeni ddos saldırılarına karşı çeşitli özellikler barındırmaktadır
- İp spoofing koruma
- Syn cookie özelliği
- Udp flood, icmp flood özellikleri
- IP başına session, paket belirleme

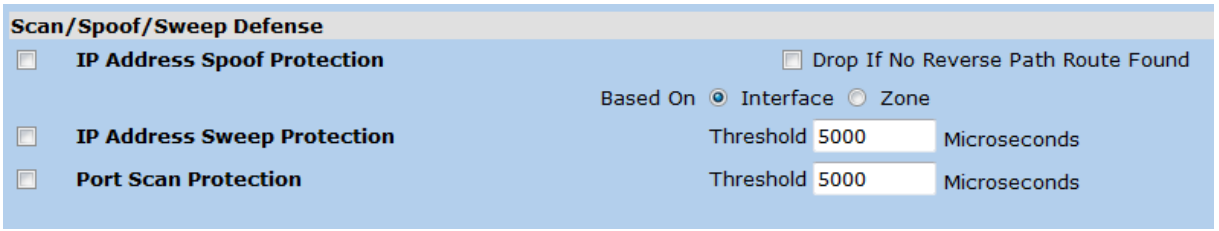
- Kandırmaya açıktır!
  - Spoof edilmiş ip adreslerinden UDP istekleri gelirse??

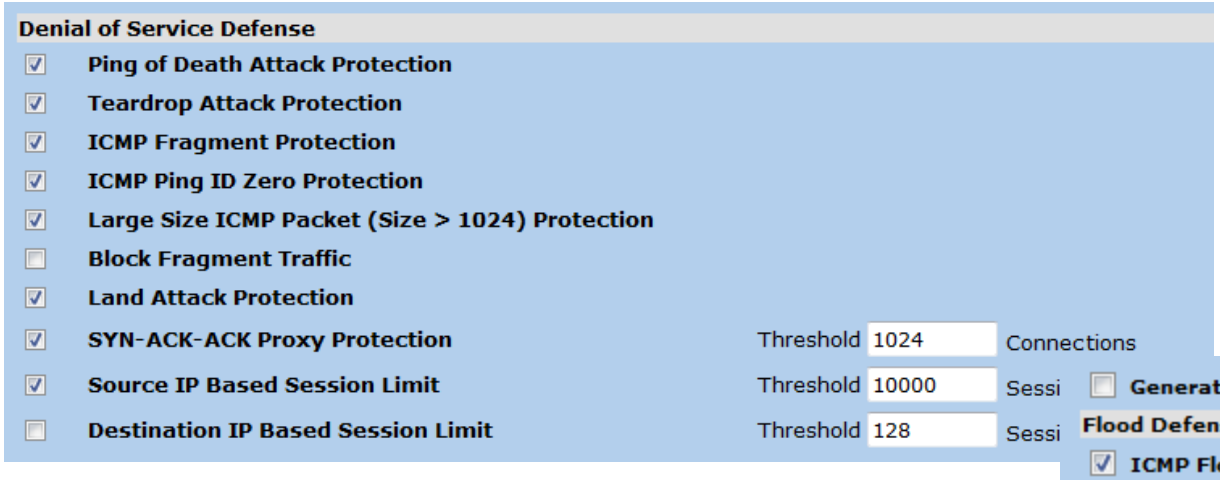
Netscreen SynCookie

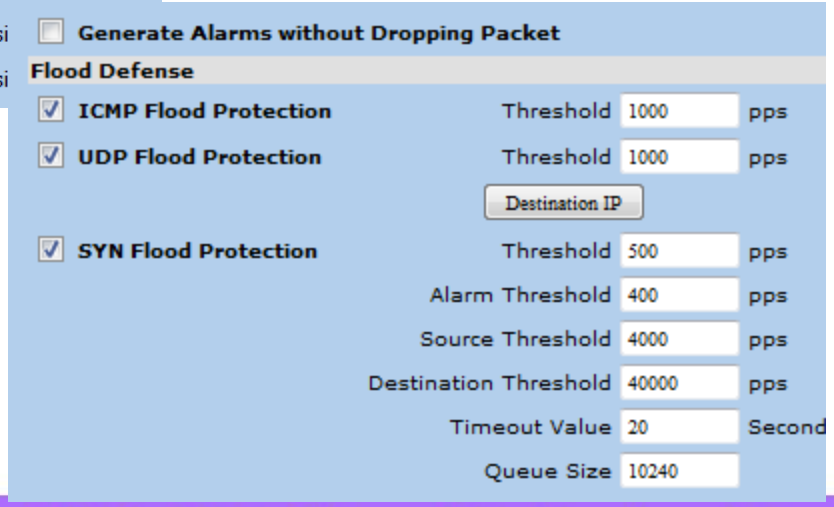
- DDOS korumasının etkili bir şekilde çalışabilmesi için öncelikle flows bölümünden TCP SYN-Proxy SYN-Cookie nin aktif edilmesi gerekir. Aksi halde aşağıda yapmış olduğumuz birçok ayar geçersiz olacaktır.



Netscreen DDoS Özellikleri



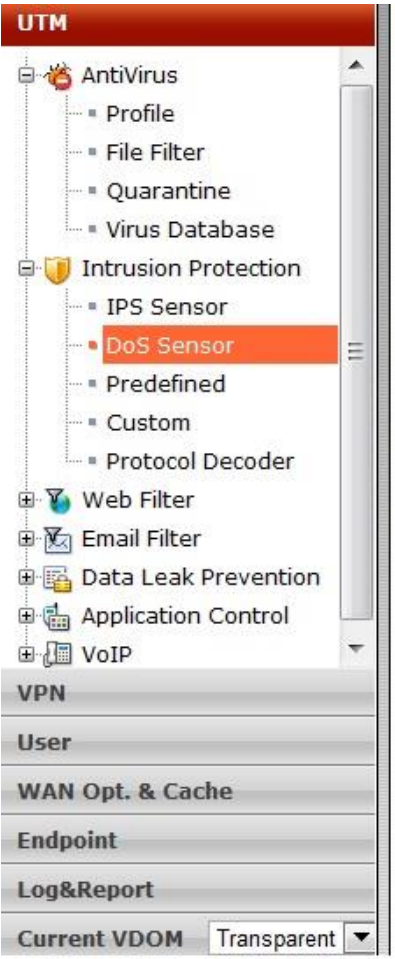




Fortinet

- Güçlü donanımsal güvenlik duvarlarından biri
- Pazar payı gün geçtikçe artmaktadır
- Alternatif güvenlik duvarlarında bulunan özelliklerin çoğunu barındırır
- Yeni sürümlerinde DDoS engelleme özellikleri de gelmektedir
- Akıllı DDoS engelleme/Botnet keşif özellikleri yoktur
- Eski ve yeni tip DDoS saldırılarını engelleyebilir

Threshold & Action Kısmı

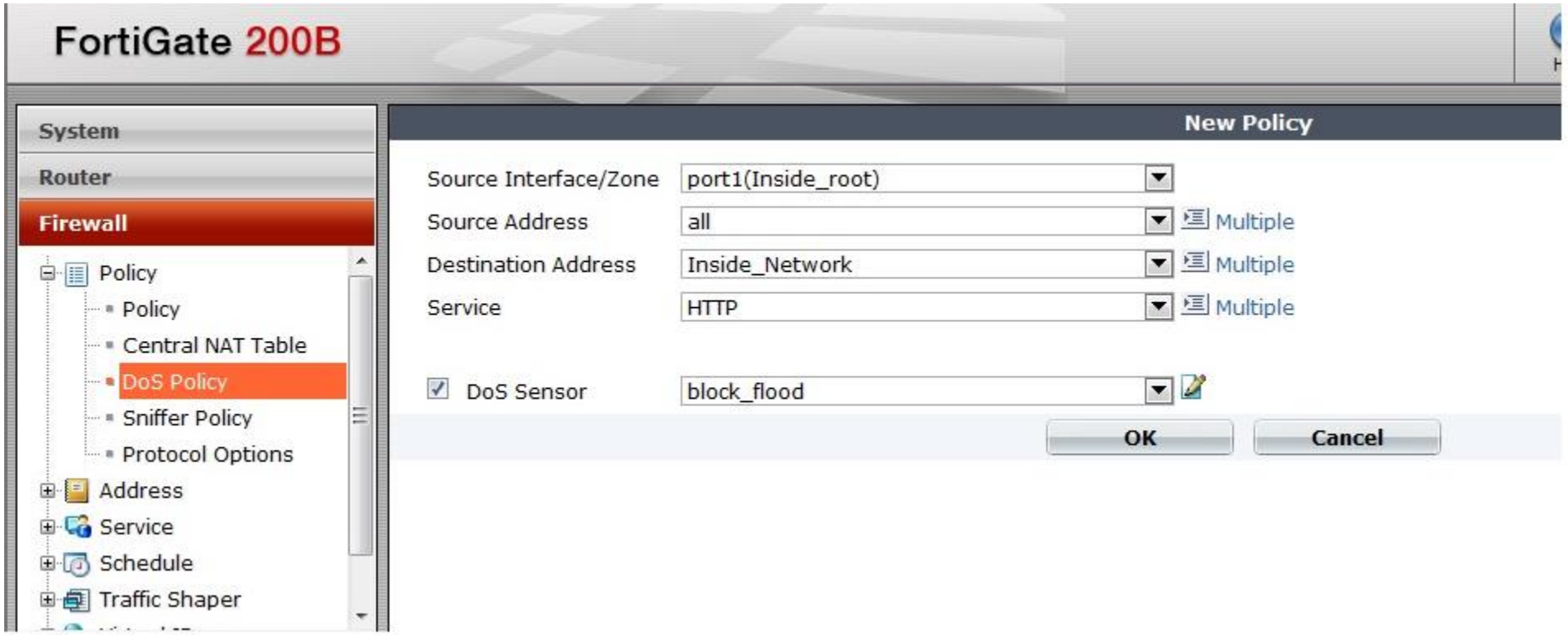


Comments (maximum 63 characters)

Anomalies Configuration:

Name	Enable	Logging	Action	Threshold
tcp_syn_flood	☑	☑	Proxy	200
tcp_port_scan	☐	☑	Block	1000
tcp_src_session	☐	☑	Block	5000
tcp_dst_session	☐	☑	Block	50000
udp_flood	☑	☑	Block	2000
udp_scan	☐	☑	Block	2000
udp_src_session	☐	☑	Block	5000
udp_dst_session	☐	☑	Block	50000
icmp_flood	☑	☑	Block	2000
icmp_sweep	☐	☑	Pass	100
icmp_src_session	☐	☑	Pass	300
icmp_dst_session	☐	☑	Pass	1000

DDoS Policy Menüsü



Özel Kartlardaki SYN Proxy Durumu

```
FGT1240B-CE4 (global) # execute npu-cli /dev/ce4_0 showsynproxy
Total Proxied TCP Connections          :        434055223
Working Proxied TCP Connections        :        515699
Retired TCP Connections                :        433539524
Valid TCP Connections                  :        0
Attacks, No Ack From Client            :        433539524
No SynAck From Server                  :        0
Rst By Server (service not supportted) :        0
Client timeout setting                 :        3 Seconds
Server timeout setting                 :        3 Seconds
```

IPS'ler ve DDoS Engelleme

- Güvenlik duvarlarına göre daha fazla seçenek sunarlar
- Uygulama seviyesi DDoS saldırıları için özel imzalar yazılabilir
  - HTTP Get Flood
  - SMTP Flood gibi...

Snort Ve DOS Saldırıları

- Snort DDOS saldırılarına karşı korumada yetersiz bir sistemdir
  - Syncookie koruma özelliği yok
  - Spoofed IP'lerden yapılan saldırılar karşısında performansı kötü
- Rate limiting yapılabilir
  - Belirli bir IP'den gelen atakları durdurabilir
  - Bot'ları engellemede kullanılabilir
- Snort yerine bu iş için en ideal çözüm olan OpenBSD/FreeBSD Packet Filter kullanılabilir.

Snort Ve DOS Saldırıları-II

- Eski tip DOS araçlarını tanır
- RBN tanır
- Kural yazılırsa GET flood , POSt Flood, DNS flood gibi uygulama seviyesi DDoS ataklarını yakalayabilir, engelleyebilir
- Synflood tanır ama engelleme modülü yok!
- Spoof edilmemiş IP adreslerinden gelen Synflood ataklarını engelleyebilir
- Udp flood engelleyebilir

Snort DOS/DDoS Kuralları

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DDOS TFN Probe"; icmp_id:678;
itype:8; content:"1234"; metadata:policy balanced-ips drop, policy security-ips drop;
reference:arachnids,443; reference:cve,2000-0138; classtype:attempted-recon; sid:221;
rev:7;)
```

```
alert tcp $HOME_NET 20432 -> $EXTERNAL_NET any (msg:"DDOS shaft client login to
handler"; flow:from_server,established; content:"login|3A|"; metadata:policy security-
ips drop; reference:arachnids,254; reference:cve,2000-0138;
reference:url,security.royans.net/info/posts/bugtraq_d...s3.shtml;
classtype:attempted-dos; sid:230; rev:7;)
```

```
# alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"DDOS shaft synflood";
flow:stateless; flags:S,12; seq:674711609; reference:cve,2000-0138;
classtype:attempted-dos; sid:241; rev:13;)
```

Snort DOS/DDoS Kuralları-II

alert udp $EXTERNAL_NET any -> $HOME_NET 31335 (msg:"DDOS Trin00 Daemon to Master message detected"; flow:to_server; content:"l44"; metadata:policy security-ips drop; reference:arachnids,186; reference:cve,2000-0138; classtype:attempted-dos; sid:231; rev:6;)

alert icmp 3.3.3.3/32 any -> $EXTERNAL_NET any (msg:"DDOS Stacheldraht server spoof"; icmp_id:666; itype:0; metadata:policy balanced-ips drop, policy security-ips drop; reference:arachnids,193; reference:cve,2000-0138; classtype:attempted-dos; sid:224; rev:6;)

Snort DOS/DDoS Kuralları-III

```
# alert udp $HOME_NET any -> $HOME_NET 67 (msg:"DOS ISC DHCP server 2 client_id length denial of service attempt"; flow:to_server; content:"c|82|Sc"; content:"= "; distance:0; metadata:policy security-ips drop; reference:cve,2006-3122; reference:url,www.debian.org/security/2006/dsa-1143; classtype:attempted-dos; sid:8056; rev:3;)
```

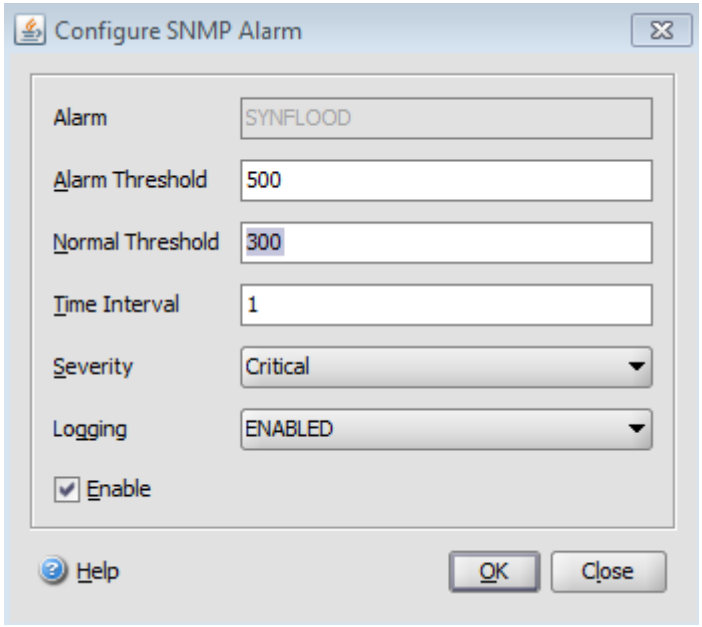
```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"DOS Apache mod_cache denial of service attempt"; flow:established, to_server; content:"Cache-Control|3A|"; nocase; pcre:"/^Cache-Control\x3A\s*(max-(age|stale)|min-fresh|s-maxage)\s*\x3D[^\d]+\x0A/smi"; reference:bugtraq,24649; reference:cve,2007-1863; classtype:denial-of-service; sid:12591; rev:1;)
```

Snort DOS/DDoS Kuralları-IV

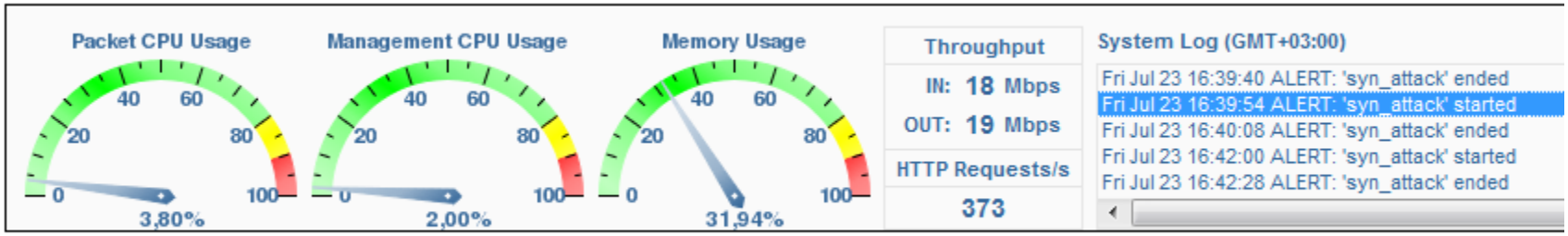
```
# alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DOS DNS root query traffic amplification attempt"; flow:to_server; content:"|00 01|"; depth:2; offset:4; content:"|00 00 02 00 01|"; within:5; distance:6; threshold:type threshold, track by_src, count 5, seconds 30; metadata:service dns; reference:url,isc.sans.org/diary.html?storyid=5713; classtype:misc-activity; sid:15259; rev:1;)
```

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET DOS Possible Slowloris Tool HTTP/Proxy Denial Of Service Attempt"; flow:to_server,established; content:"GET /"; depth:5; content:"User-Agent\: Mozilla/4.0 (compatible\; MSIE 7.0\; Windows NT 5.1\; Trident/4.0"; offset:30; depth:90; threshold: type threshold, track by_src, count 100, seconds 30; classtype:attempted-dos; reference:url,isc.sans.org/diary.html?storyid=6601; reference:url,www.packetstormsecurity.com/filedesc/slowloris.pl.txt.html; reference:url,doc.emergingthreats.net/2009413; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Slowliris; sid:2009413; rev:2;)
```

Citrix Netscaler



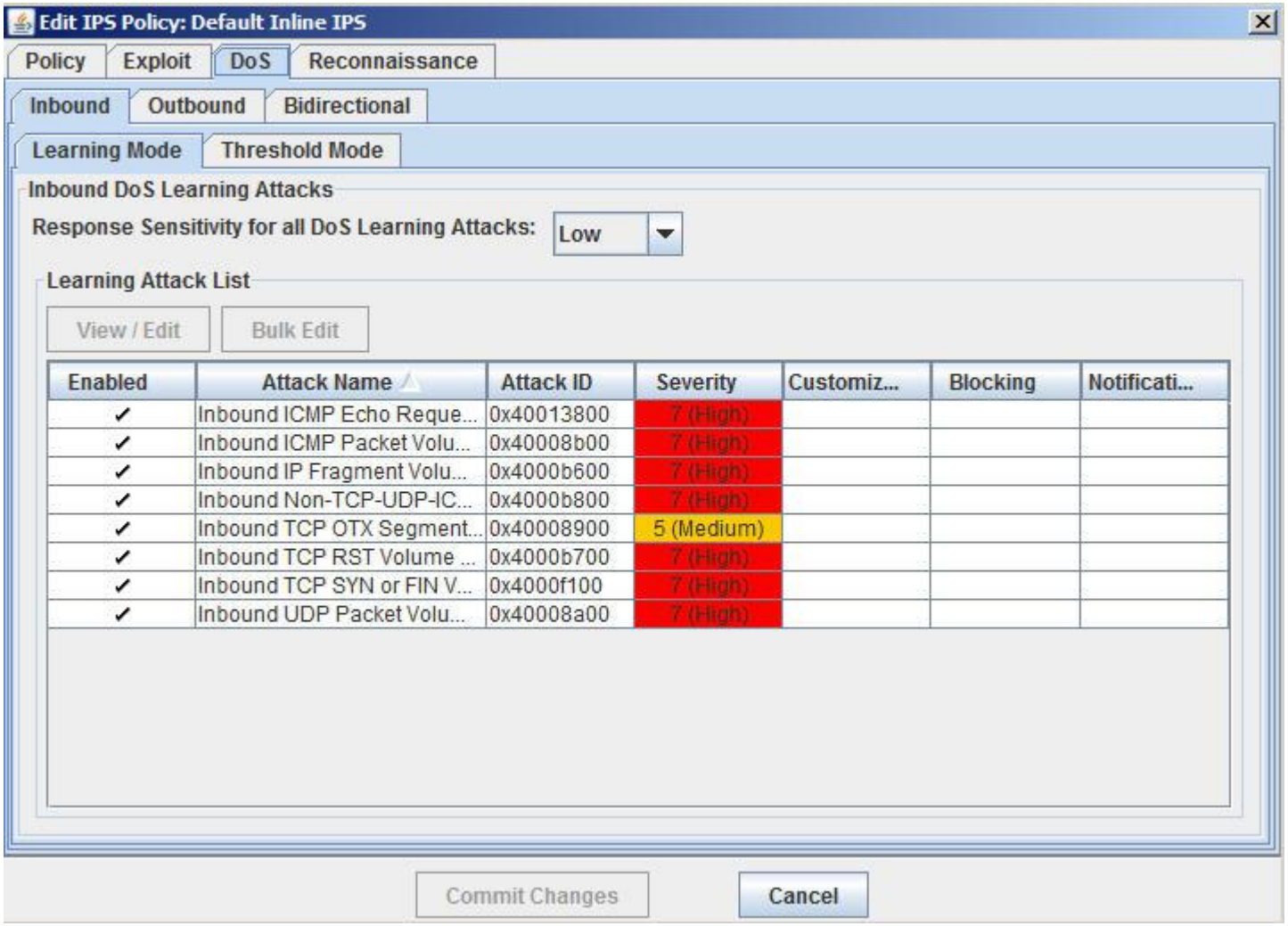
- Güçlü SYN Flood koruma özelliği
- Güçlü HTTP Flood koruma özelliği
- Diğer DDoS tiplerine karşı koruması yoktur



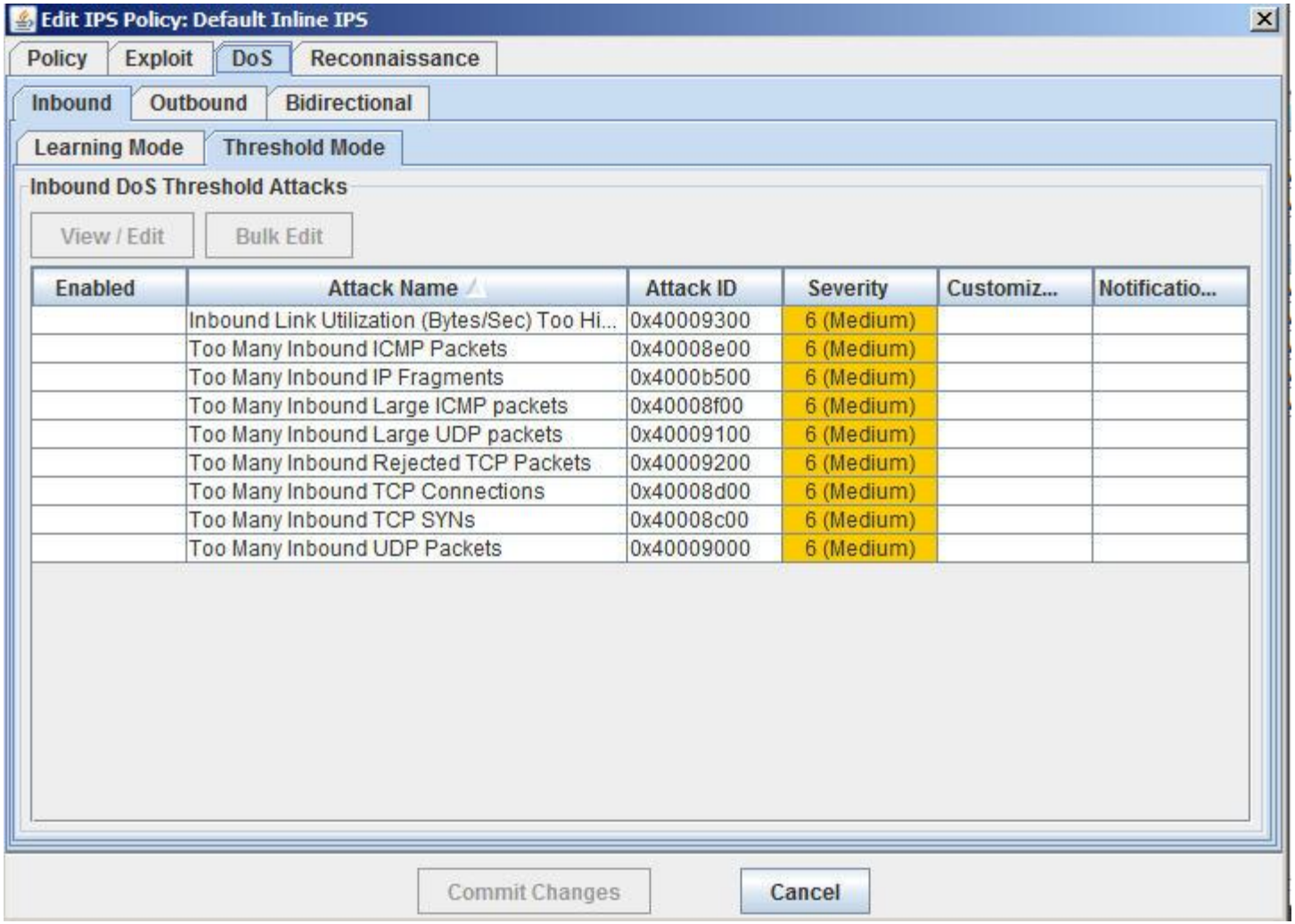
McAfee Intrushield

- DDoS konusunda özellik bakımından en gerçekçi IPS
- DDoS özelliklerinin çoğu istatistiksel bilgiye dayanıyor
- İyi ayarlanmazsa false positive oranı ciddi miktarda olup rahatsız edebiliyor
- Syn cookie özelliği iyi çalışır
- Rate limiting özellikleri

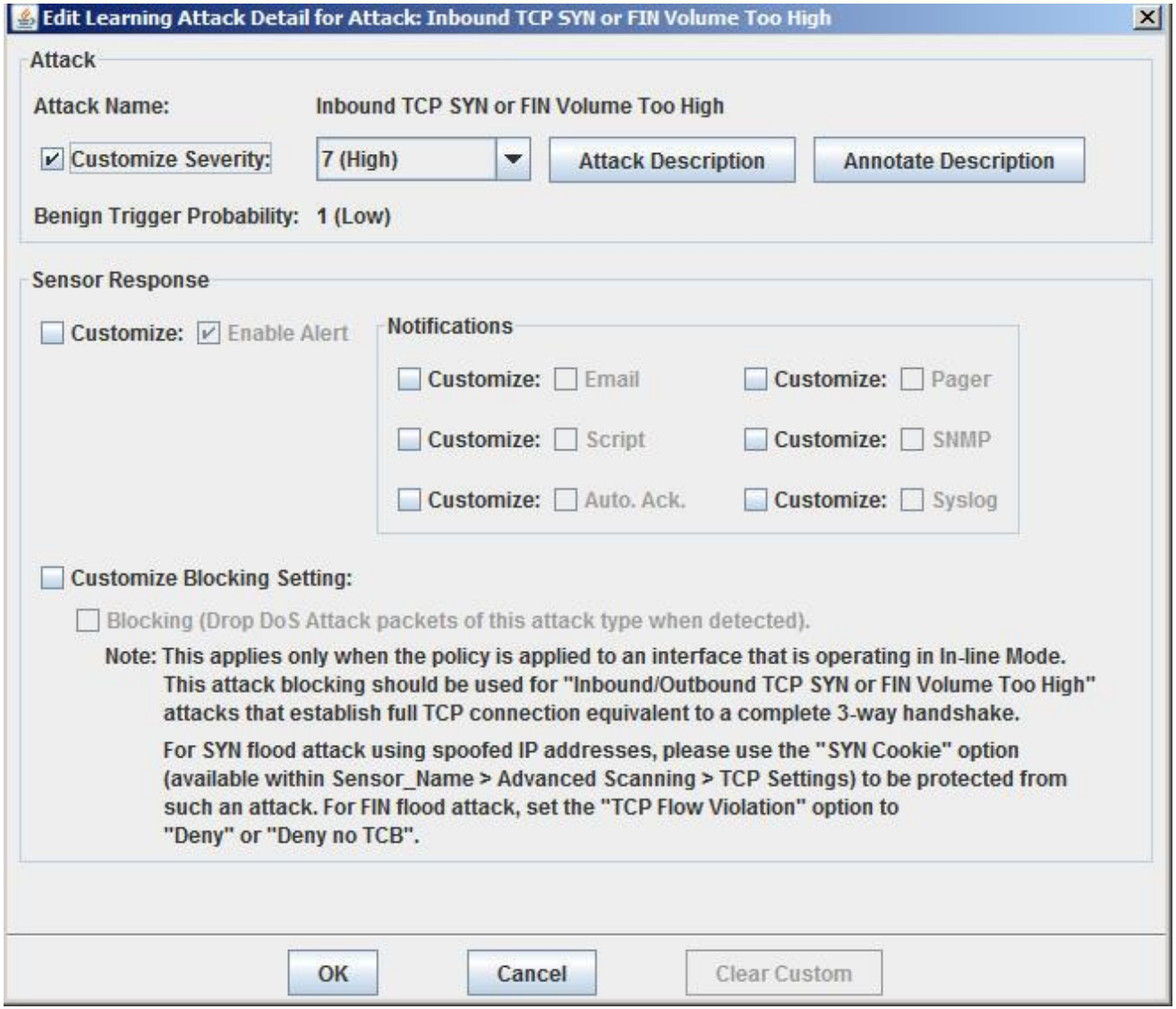
McAfee-I


Edit IPS Policy: Default Inline IPS
Policy
Exploit
DoS
Reconnaissance
Inbound
Outbound
Bidirectional
Learning Mode
Threshold Mode
Inbound DoS Learning Attacks
Response Sensitivity for all DoS Learning Attacks:
Low
Learning Attack List
View / Edit
Bulk Edit
Enabled
Attack Name
Attack ID
Severity
Customiz...
Blocking
Notificati...
✓ Inbound ICMP Echo Reque... 0x40013800 7 (High)
✓ Inbound ICMP Packet Volu... 0x40008b00 7 (High)
✓ Inbound IP Fragment Volu... 0x4000b600 7 (High)
✓ Inbound Non-TCP-UDP-IC... 0x4000b800 7 (High)
✓ Inbound TCP OTX Segment... 0x40008900 5 (Medium)
✓ Inbound TCP RST Volume ... 0x4000b700 7 (High)
✓ Inbound TCP SYN or FIN V... 0x4000f100 7 (High)
✓ Inbound UDP Packet Volu... 0x40008a00 7 (High)
Commit Changes
Cancel

McAfee-II


Edit IPS Policy: Default Inline IPS
Policy
Exploit
DoS
Reconnaissance
Inbound
Outbound
Bidirectional
Learning Mode
Threshold Mode
Inbound DoS Threshold Attacks
View / Edit
Bulk Edit
Enabled
Attack Name
Attack ID
Severity
Customiz...
Notificatio...
Inbound Link Utilization (Bytes/Sec) Too Hi... 0x40009300 6 (Medium)
Too Many Inbound ICMP Packets 0x40008e00 6 (Medium)
Too Many Inbound IP Fragments 0x4000b500 6 (Medium)
Too Many Inbound Large ICMP packets 0x40008f00 6 (Medium)
Too Many Inbound Large UDP packets 0x40009100 6 (Medium)
Too Many Inbound Rejected TCP Packets 0x40009200 6 (Medium)
Too Many Inbound TCP Connections 0x40008d00 6 (Medium)
Too Many Inbound TCP SYNs 0x40008c00 6 (Medium)
Too Many Inbound UDP Packets 0x40009000 6 (Medium)
Commit Changes
Cancel

McAfee-III

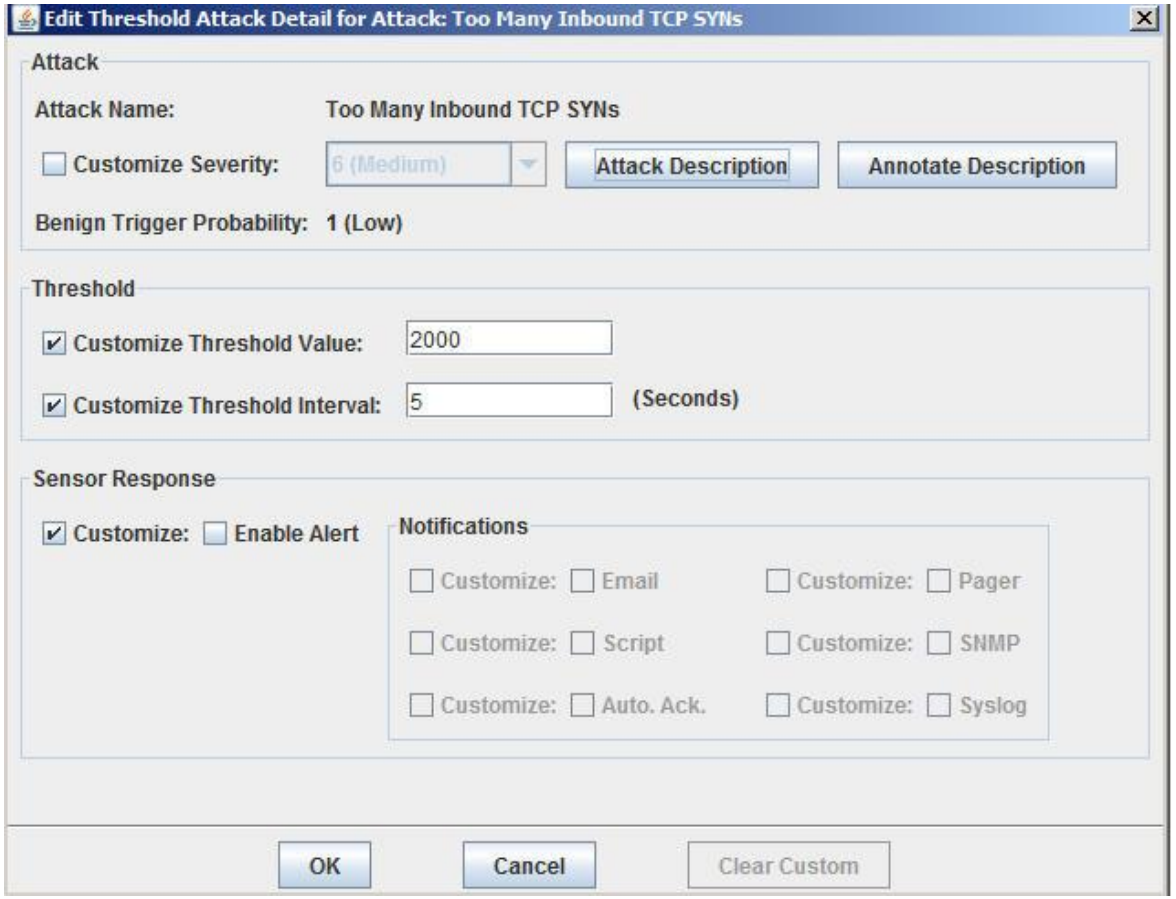

Edit Learning Attack Detail for Attack: Inbound TCP SYN or FIN Volume Too High
Attack
Attack Name:
Inbound TCP SYN or FIN Volume Too High
Customize Severity:
7 (High)
Attack Description
Annotate Description
Benign Trigger Probability:
1 (Low)
Sensor Response
Customize:
Enable Alert
Notifications
Customize:
Email
Customize:
Pager
Customize:
Script
Customize:
SNMP
Customize:
Auto. Ack.
Customize:
Syslog
Customize Blocking Setting:
Blocking (Drop DoS Attack packets of this attack type when detected).
Note: This applies only when the policy is applied to an interface that is operating in In-line Mode.
This attack blocking should be used for "Inbound/Outbound TCP SYN or FIN Volume Too High"
attacks that establish full TCP connection equivalent to a complete 3-way handshake.
For SYN flood attack using spoofed IP addresses, please use the "SYN Cookie" option
(available within Sensor_Name > Advanced Scanning > TCP Settings) to be protected from
such an attack. For FIN flood attack, set the "TCP Flow Violation" option to
"Deny" or "Deny no TCB".
OK
Cancel
Clear Custom

Rate limiting dezavantajları

- Akıllı saldırganın en sevdiği koruma yöntemidir☺
- Neden ?

#Hping –a root_dnsler www.hedefsistem.com –flood –S –p 80

☺☺

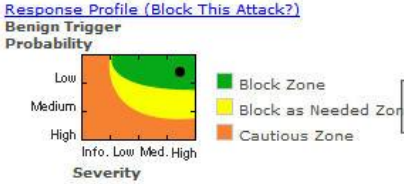


Attack Information & Description

Inbound TCP SYN or FIN Volume Too High

Vulnerability Type:	Brute Force
Impact Category:	VolumeDoS
Impact Subcategory:	Statistical Deviation
Severity:	High
Benign Trigger Probability:	Low

Response Profile (Block This Attack?)



Description

This alert indicates a possible DDoS attack based on a large number of TCP SYN or FIN packets. The basic SYN or FIN flood attack works by sending a high volume of SYN or FIN packets to the target host, and then never responding to the packets that are returned, thus filling up the data structure(s) used by the target host to keep track of pending connections. Although pending connections will time out eventually and free up space in the data structure(s), the sender can simply transmit additional SYN or FIN packets faster than they can expire. Specifically, this event correlated with another event (TCP Control Segment Anomaly) should provide a more accurate picture of the current event. If this alert is see along with "TCP Control Segment Anomaly" alert, you are likely under a SYN or FIN flood attack; If this alert is seen without the "TCP Control Segment Anomaly" alert, there is likely a flash-crowd condition in your network but it does not seem to affect the performance of the TCP-based servers yet. If "TCP Control Segment Anomaly" alert is seen without this alert, there could be a sudden change in the network routes or some TCP-based servers may become slow.

Possible Effects

Internet-connected networks supporting TCP-based services may experience service problems while under attack, as well as for an indefinite period of time after the attack ceases (until the issue is resolved). The server itself is not harme by the attack; usually only the ability to provide the service is impaired. In some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

Recommended Solution

Response Actions:

One measure for preventing spoofing attacks is to install a filtering router. This router should restrict inbound external traffic that claims to be originating from within your internal network. In addition, you should filter outgoing packets tha have a source address different from your internal network to prevent a source IP spoofing attack from originating from your site.

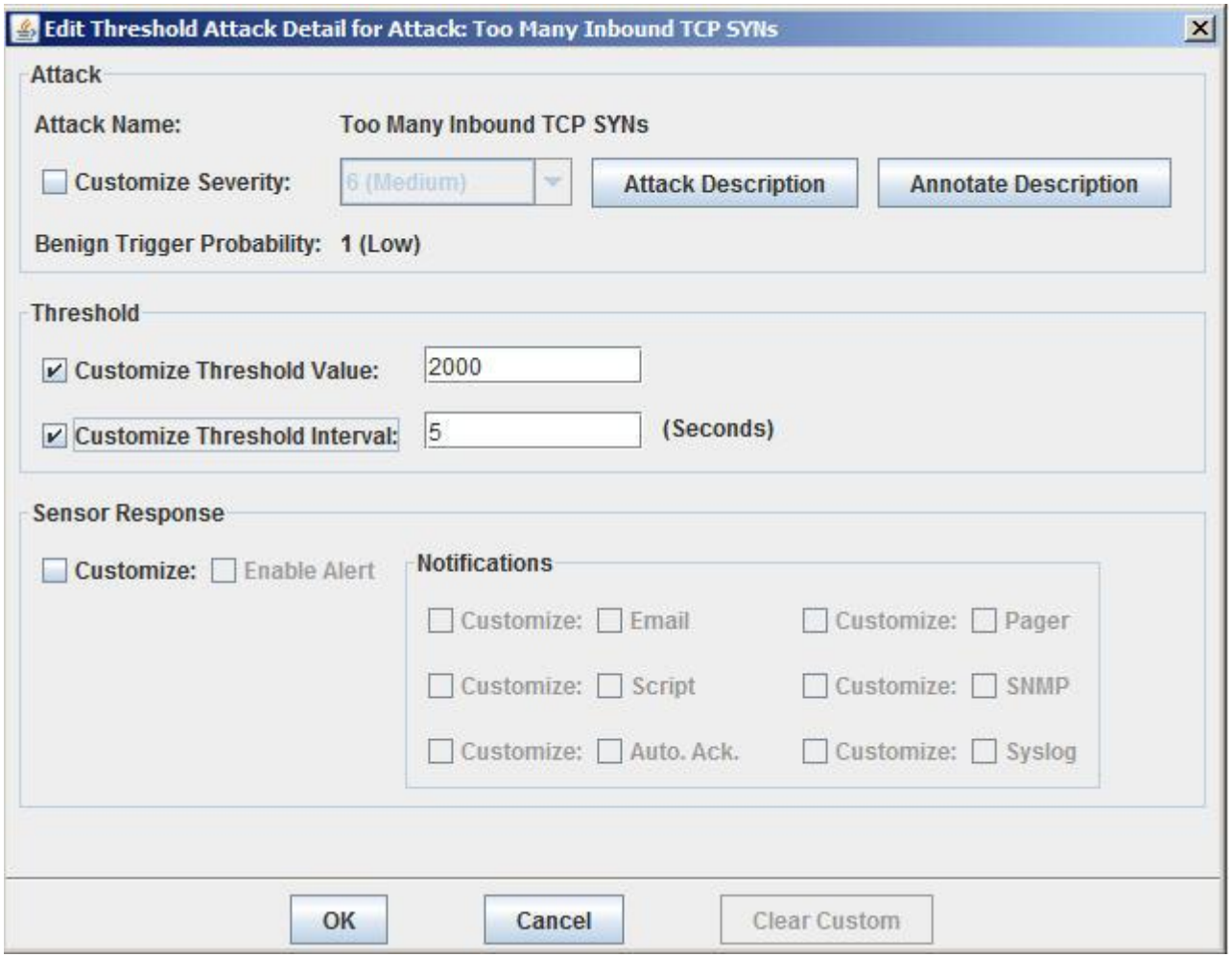
Platforms Affected

Software Packages

any Internet connected machine

Reference

Intruvert ID:	0x4000f100
Content Updated:	12-12-2005
Target Release Date:	
CVE:	CVE-2002-1712


Edit Threshold Attack Detail for Attack: Too Many Inbound TCP SYNs
Attack
Attack Name:
Too Many Inbound TCP SYNs
Customize Severity:
6 (Medium)
Attack Description
Annotate Description
Benign Trigger Probability:
1 (Low)
Threshold
Customize Threshold Value:
2000
Customize Threshold Interval:
5
(Seconds)
Sensor Response
Customize:
Enable Alert
Notifications
Customize:
Email
Customize:
Pager
Customize:
Script
Customize:
SNMP
Customize:
Auto. Ack.
Customize:
Syslog
OK
Cancel
Clear Custom

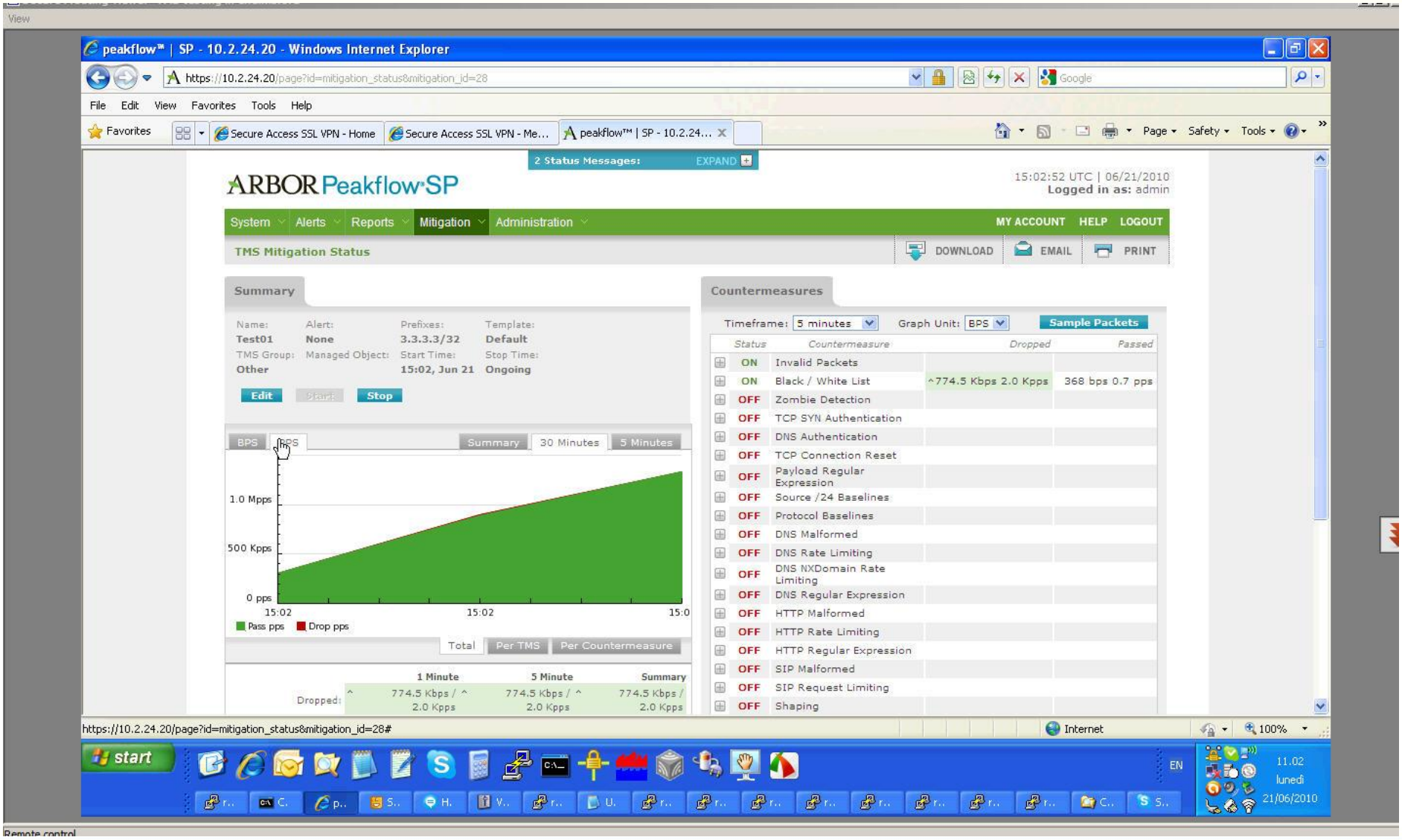
SourceFire

- Snort ile aynı özelliklere sahiptir
- Syn flood DDoS saldırılarında işe yaramaz
- Diğer DDoS saldırıları için güçlü bir altyapı sunar

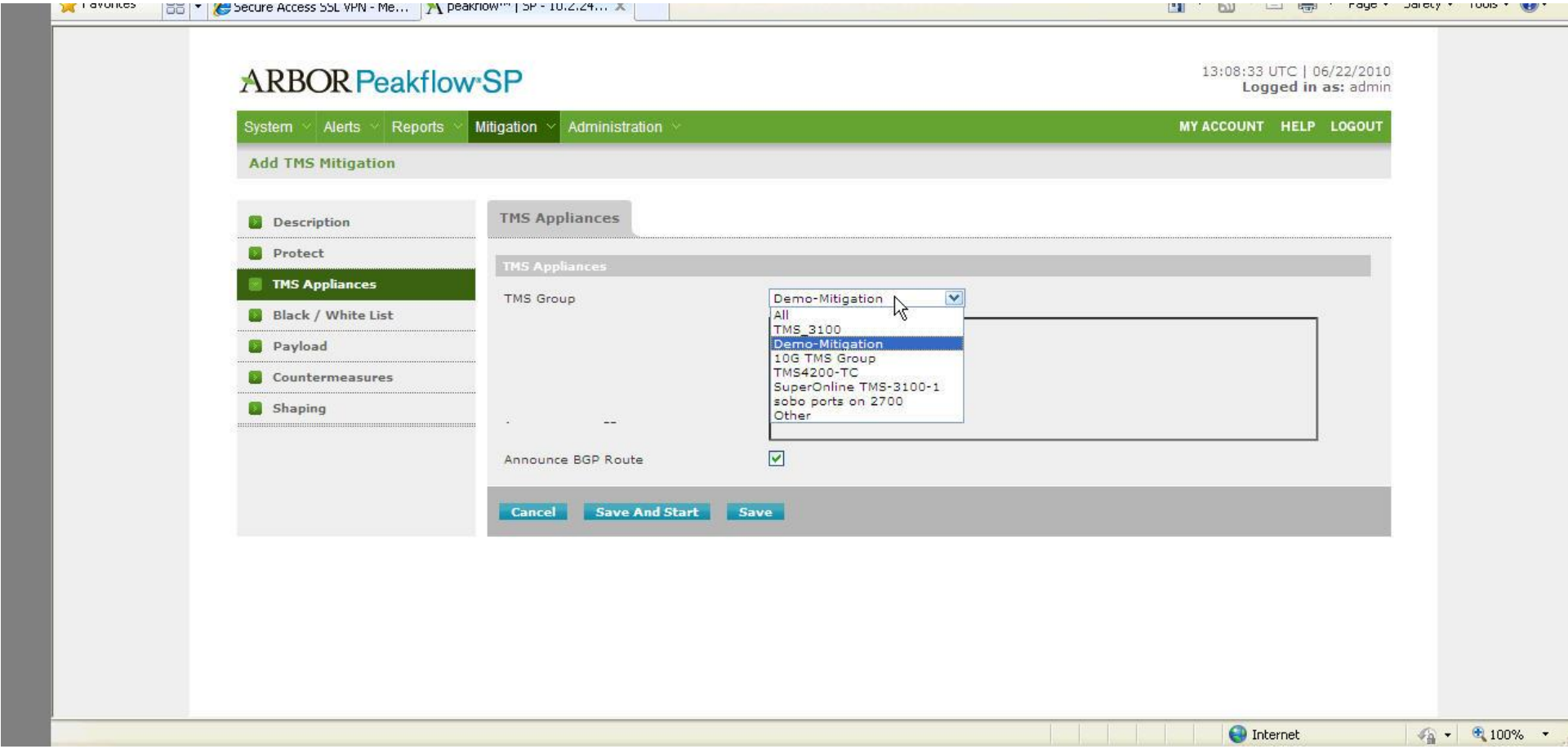
Arbor

- Internette en falza tercih edilen DDoS engelleme ürünü
- 2002- ...
- DDoS konusunda özel yetişmiş elemanlara sahiptir
  - DDoS istatistikleri yayınlayan nadir firmalardan
- Tabanında Linux&OpenBSD kullanır
- Hemen her tür DDoS saldırılarını engelleyebilir
- Daha çok Inline değil ISP'lerder konumlandırılır
  - BGP ile saldırı anında trafiği üzerine alarak temizleme işlemi yapar.

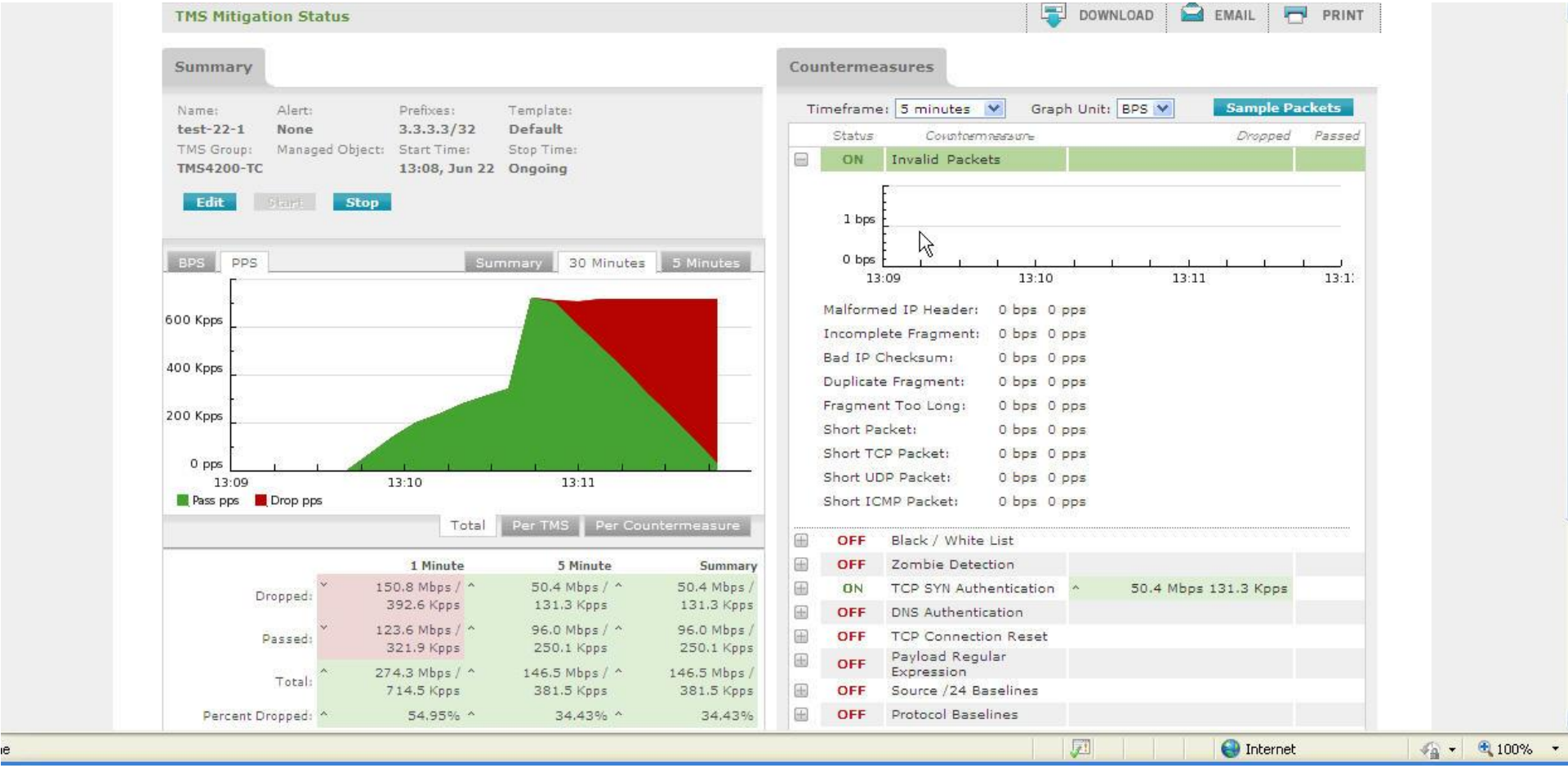
PeakFlow DDoS Koruma Özellikleri



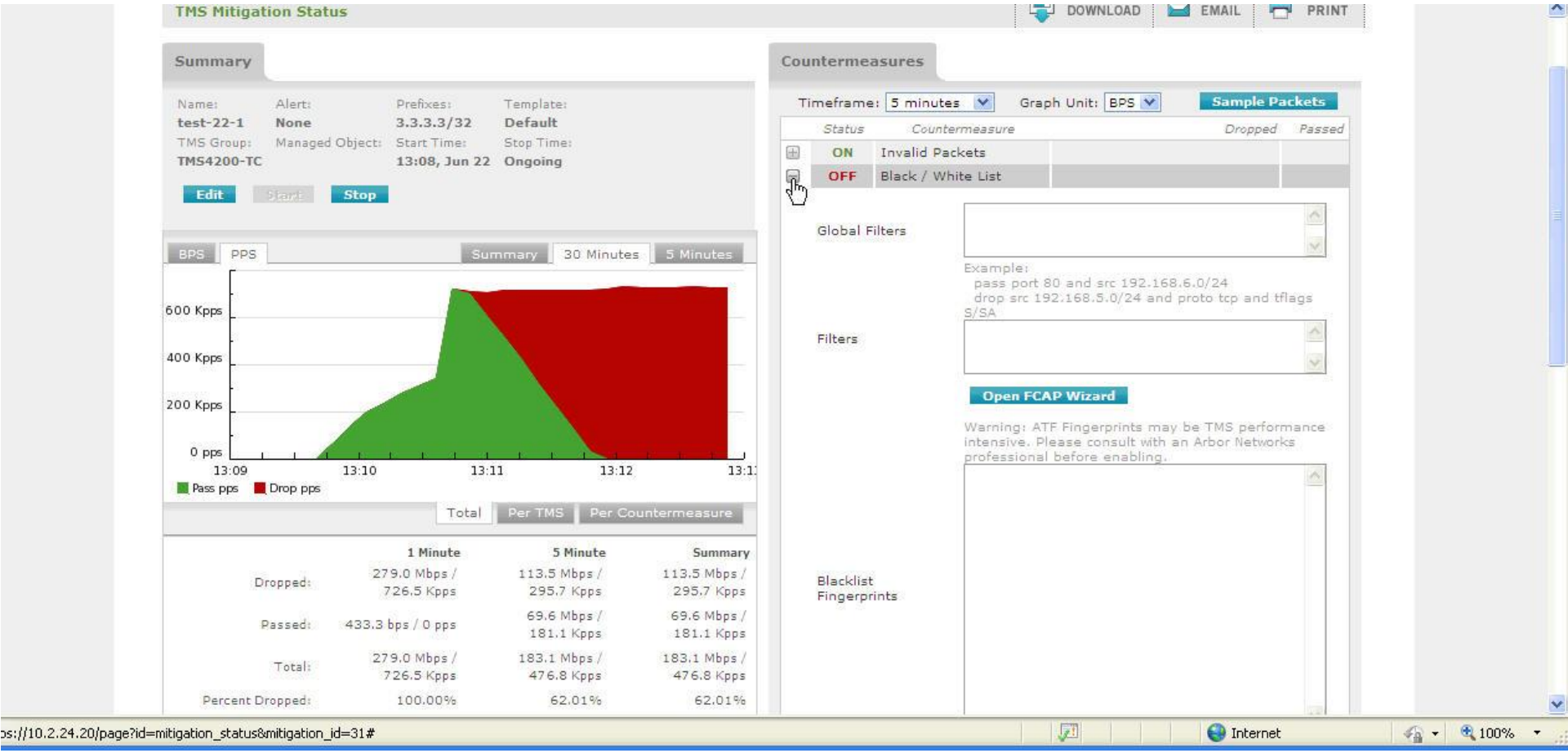
Arbor-I


ARBOR Peakflow SP
13:08:33 UTC | 06/22/2010
Logged in as: admin
System
Alerts
Reports
Mitigation
Administration
MY ACCOUNT
HELP
LOGOUT
Add TMS Mitigation
Description
Protect
TMS Appliances
Black / White List
Payload
Countermeasures
Shaping
TMS Appliances
TMS Appliances
TMS Group
Demo-Mitigation
All
TMS_3100
Demo-Mitigation
10G TMS Group
TMS4200-TC
SuperOnline TMS-3100-1
sobo ports on 2700
Other
Announce BGP Route
Cancel
Save And Start
Save
Internet
100%

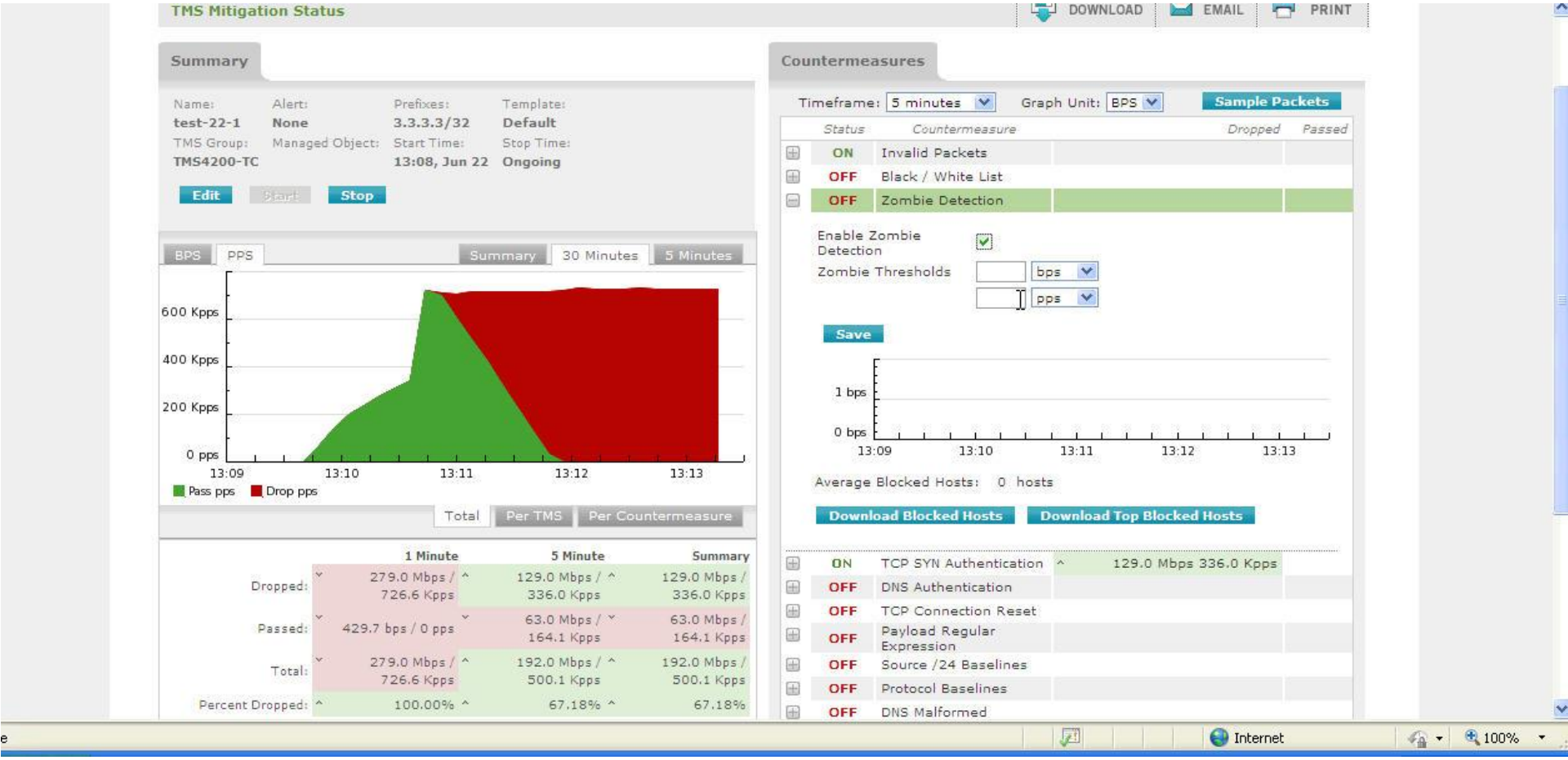
Arbor-II


TMS Mitigation Status
DOWNLOAD
EMAIL
PRINT
Summary
Name: test-22-1
Alert: None
Prefixes: 3.3.3.3/32
Template: Default
TMS Group: TMS4200-TC
Managed Object:
Start Time: 13:08, Jun 22
Stop Time: Ongoing
Edit
Start
Stop
BPS
PPS
Summary
30 Minutes
5 Minutes
600 Kpps
400 Kpps
200 Kpps
0 pps
13:09
13:10
13:11
Pass pps
Drop pps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 150.8 Mbps / 392.6 Kpps | 50.4 Mbps / 131.3 Kpps | 50.4 Mbps / 131.3 Kpps
Passed: 123.6 Mbps / 321.9 Kpps | 96.0 Mbps / 250.1 Kpps | 96.0 Mbps / 250.1 Kpps
Total: 274.3 Mbps / 714.5 Kpps | 146.5 Mbps / 381.5 Kpps | 146.5 Mbps / 381.5 Kpps
Percent Dropped: 54.95% | 34.43% | 34.43%
Countermeasures
Timeframe: 5 minutes
Graph Unit: BPS
Sample Packets
Status
Countermeasure
Dropped
Passed
ON Invalid Packets
1 bps
0 bps
13:09
13:10
13:11
Malformed IP Header: 0 bps 0 pps
Incomplete Fragment: 0 bps 0 pps
Bad IP Checksum: 0 bps 0 pps
Duplicate Fragment: 0 bps 0 pps
Fragment Too Long: 0 bps 0 pps
Short Packet: 0 bps 0 pps
Short TCP Packet: 0 bps 0 pps
Short UDP Packet: 0 bps 0 pps
Short ICMP Packet: 0 bps 0 pps
OFF Black / White List
OFF Zombie Detection
ON TCP SYN Authentication 50.4 Mbps 131.3 Kpps
OFF DNS Authentication
OFF TCP Connection Reset
OFF Payload Regular Expression
OFF Source /24 Baselines
OFF Protocol Baselines
Internet
100%

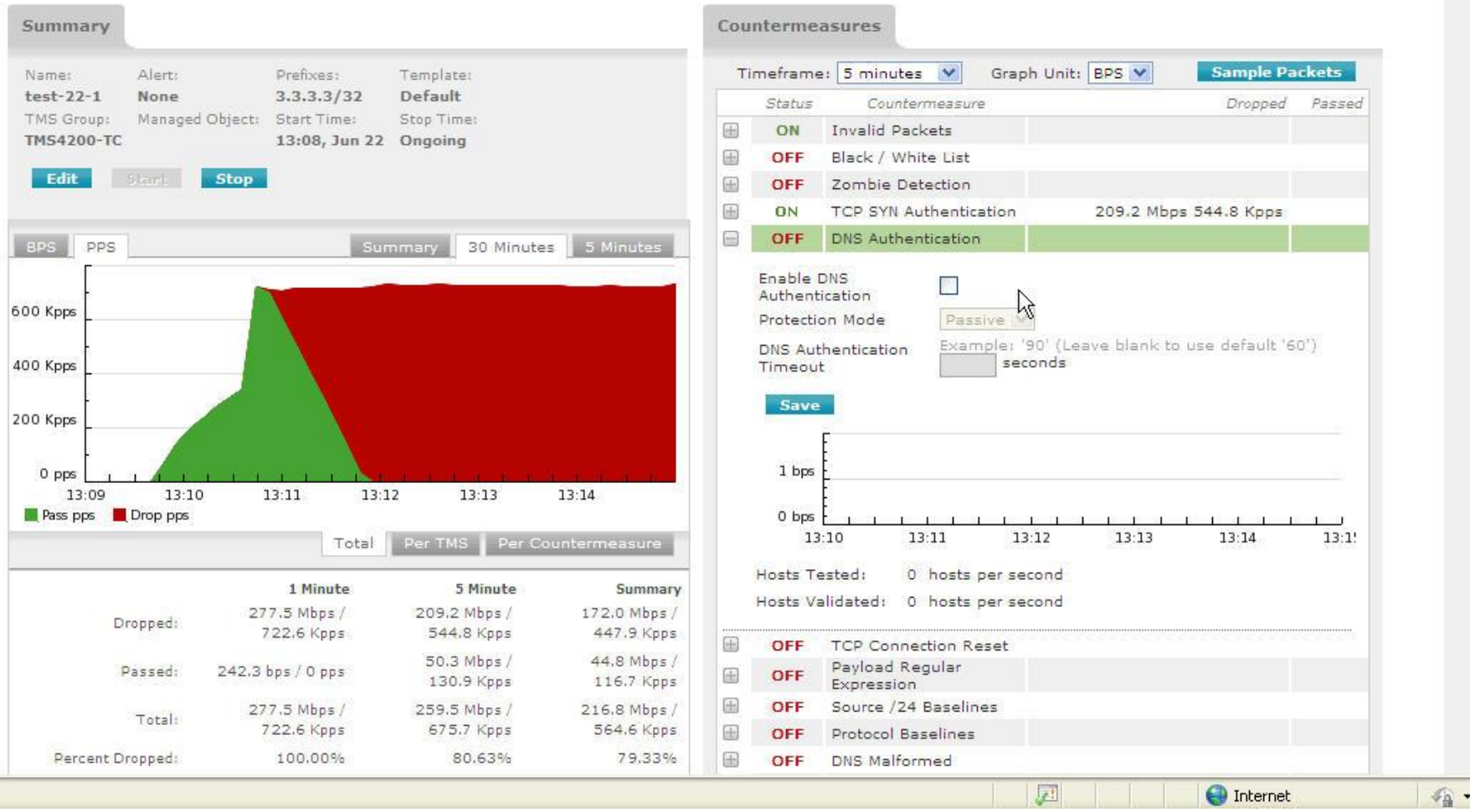
Arbor-III


TMS Mitigation Status
DOWNLOAD
EMAIL
PRINT
Summary
Name: test-22-1
Alert: None
Prefixes: 3.3.3.3/32
Template: Default
TMS Group: TMS4200-TC
Managed Object:
Start Time: 13:08, Jun 22
Stop Time: Ongoing
Edit
Start
Stop
BPS
PPS
Summary
30 Minutes
5 Minutes
600 Kpps
400 Kpps
200 Kpps
0 pps
13:09
13:10
13:11
13:12
Pass pps
Drop pps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 279.0 Mbps / 726.5 Kpps | 113.5 Mbps / 295.7 Kpps | 113.5 Mbps / 295.7 Kpps
Passed: 433.3 bps / 0 pps | 69.6 Mbps / 181.1 Kpps | 69.6 Mbps / 181.1 Kpps
Total: 279.0 Mbps / 726.5 Kpps | 183.1 Mbps / 476.8 Kpps | 183.1 Mbps / 476.8 Kpps
Percent Dropped: 100.00% | 62.01% | 62.01%
Countermeasures
Timeframe: 5 minutes
Graph Unit: BPS
Sample Packets
Status
Countermeasure
Dropped
Passed
ON
Invalid Packets
OFF
Black / White List
Global Filters
Example:
pass port 80 and src 192.168.6.0/24
drop src 192.168.5.0/24 and proto tcp and tflags S/SA
Filters
Open FCAP Wizard
Warning: ATF Fingerprints may be TMS performance intensive. Please consult with an Arbor Networks professional before enabling.
Blacklist Fingerprints
https://10.2.24.20/page?id=mitigation_status&mitigation_id=31#
Internet
100%

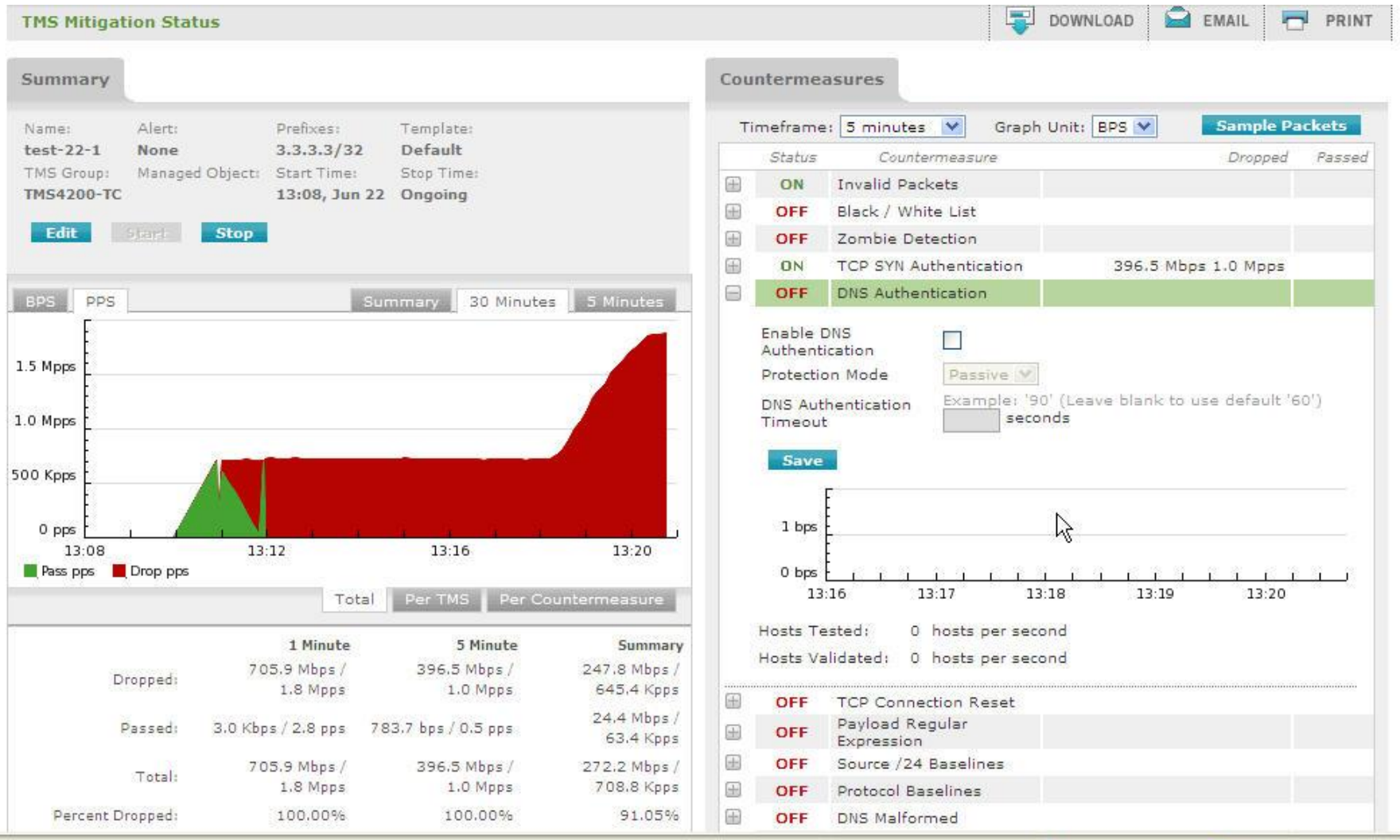
Arbor-IV


TMS Mitigation Status
DOWNLOAD
EMAIL
PRINT
Summary
Name: test-22-1
Alert: None
Prefixes: 3.3.3.3/32
Template: Default
TMS Group: TMS4200-TC
Managed Object:
Start Time: 13:08, Jun 22
Stop Time: Ongoing
Edit
Start
Stop
BPS
PPS
Summary
30 Minutes
5 Minutes
600 Kpps
400 Kpps
200 Kpps
0 pps
13:09
13:10
13:11
13:12
13:13
Pass pps
Drop pps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 279.0 Mbps / 726.6 Kpps | 129.0 Mbps / 336.0 Kpps | 129.0 Mbps / 336.0 Kpps
Passed: 429.7 bps / 0 pps | 63.0 Mbps / 164.1 Kpps | 63.0 Mbps / 164.1 Kpps
Total: 279.0 Mbps / 726.6 Kpps | 192.0 Mbps / 500.1 Kpps | 192.0 Mbps / 500.1 Kpps
Percent Dropped: 100.00% | 67.18% | 67.18%
Countermeasures
Timeframe: 5 minutes
Graph Unit: BPS
Sample Packets
Status
Countermeasure
Dropped
Passed
ON Invalid Packets
OFF Black / White List
OFF Zombie Detection
Enable Zombie Detection
Zombie Thresholds
bps
pps
Save
1 bps
0 bps
13:09
13:10
13:11
13:12
13:13
Average Blocked Hosts: 0 hosts
Download Blocked Hosts
Download Top Blocked Hosts
ON TCP SYN Authentication 129.0 Mbps 336.0 Kpps
OFF DNS Authentication
OFF TCP Connection Reset
OFF Payload Regular Expression
OFF Source /24 Baselines
OFF Protocol Baselines
OFF DNS Malformed
Internet
100%

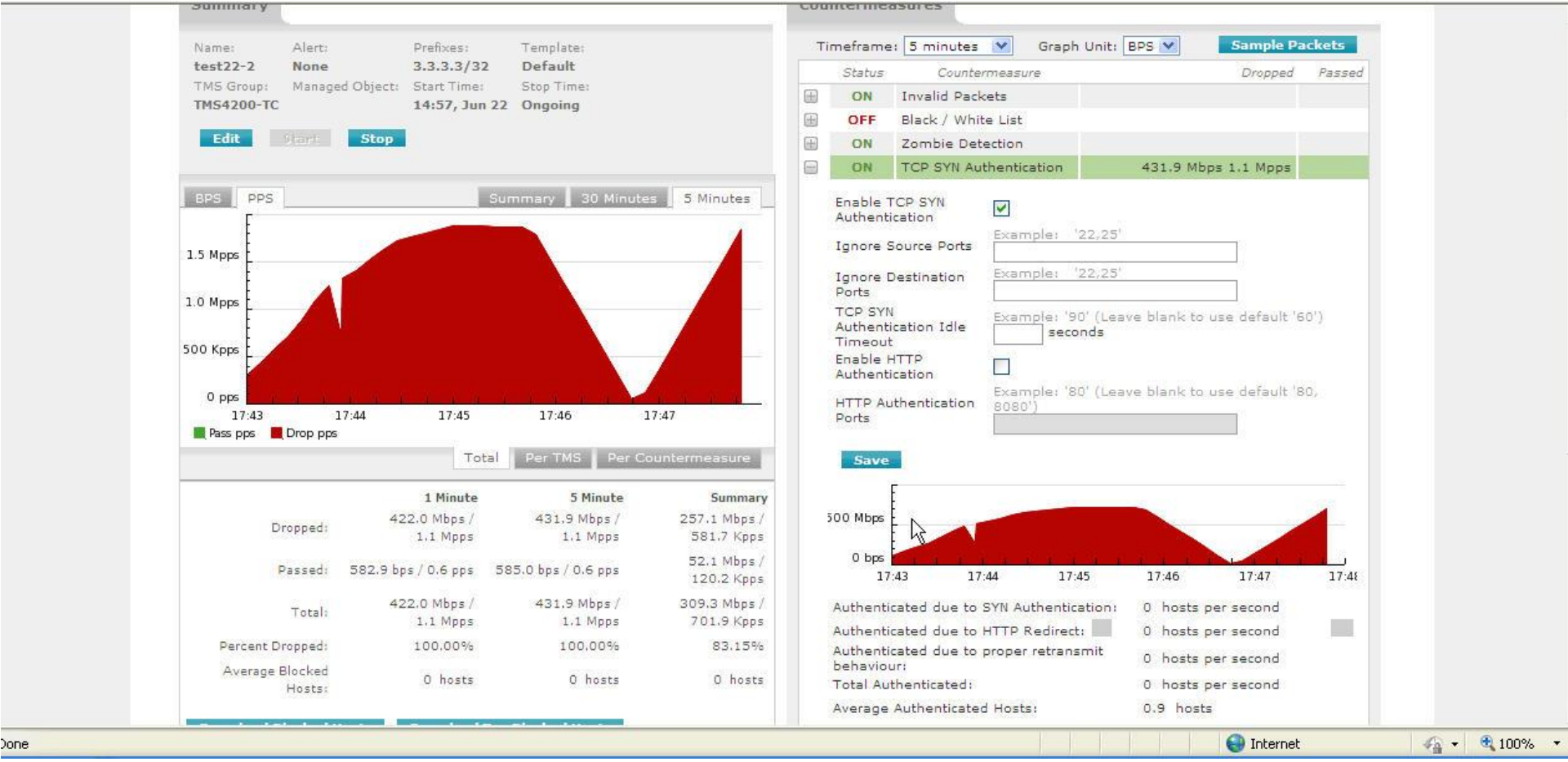
Arbor-V


Summary
Name: test-22-1
Alert: None
Prefixes: 3.3.3.3/32
Template: Default
TMS Group: TMS4200-TC
Managed Object:
Start Time: 13:08, Jun 22
Stop Time: Ongoing
Edit
Start
Stop
BPS
PPS
Summary
30 Minutes
5 Minutes
600 Kpps
400 Kpps
200 Kpps
0 pps
13:09
13:10
13:11
13:12
13:13
13:14
Pass pps
Drop pps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 277.5 Mbps / 722.6 Kpps | 209.2 Mbps / 544.8 Kpps | 172.0 Mbps / 447.9 Kpps
Passed: 242.3 bps / 0 pps | 50.3 Mbps / 130.9 Kpps | 44.8 Mbps / 116.7 Kpps
Total: 277.5 Mbps / 722.6 Kpps | 259.5 Mbps / 675.7 Kpps | 216.8 Mbps / 564.6 Kpps
Percent Dropped: 100.00% | 80.63% | 79.33%
Countermeasures
Timeframe: 5 minutes
Graph Unit: BPS
Sample Packets
Status
Countermeasure
Dropped
Passed
ON Invalid Packets
OFF Black / White List
OFF Zombie Detection
ON TCP SYN Authentication 209.2 Mbps 544.8 Kpps
OFF DNS Authentication
Enable DNS Authentication
Protection Mode
Passive
DNS Authentication Timeout
Example: '90' (Leave blank to use default '60')
seconds
Save
1 bps
0 bps
13:10
13:11
13:12
13:13
13:14
Hosts Tested: 0 hosts per second
Hosts Validated: 0 hosts per second
OFF TCP Connection Reset
OFF Payload Regular Expression
OFF Source /24 Baselines
OFF Protocol Baselines
OFF DNS Malformed
Internet

Arbor-VI


TMS Mitigation Status
DOWNLOAD
EMAIL
PRINT
Summary
Name: test-22-1
Alert: None
Prefixes: 3.3.3.3/32
Template: Default
TMS Group: TMS4200-TC
Managed Object:
Start Time: 13:08, Jun 22
Stop Time: Ongoing
Edit
Start
Stop
BPS
PPS
Summary
30 Minutes
5 Minutes
1.5 Mpps
1.0 Mpps
500 Kpps
0 pps
13:08
13:12
13:16
13:20
Pass pps
Drop pps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 705.9 Mbps / 1.8 Mpps | 396.5 Mbps / 1.0 Mpps | 247.8 Mbps / 645.4 Kpps
Passed: 3.0 Kbps / 2.8 pps | 783.7 bps / 0.5 pps | 24.4 Mbps / 63.4 Kpps
Total: 705.9 Mbps / 1.8 Mpps | 396.5 Mbps / 1.0 Mpps | 272.2 Mbps / 708.8 Kpps
Percent Dropped: 100.00% | 100.00% | 91.05%
Countermeasures
Timeframe: 5 minutes
Graph Unit: BPS
Sample Packets
Status
Countermeasure
Dropped
Passed
ON Invalid Packets
OFF Black / White List
OFF Zombie Detection
ON TCP SYN Authentication 396.5 Mbps 1.0 Mpps
OFF DNS Authentication
Enable DNS Authentication
Protection Mode
Passive
DNS Authentication Timeout
Example: '90' (Leave blank to use default '60')
seconds
Save
1 bps
0 bps
13:16
13:17
13:18
13:19
13:20
Hosts Tested: 0 hosts per second
Hosts Validated: 0 hosts per second
OFF TCP Connection Reset
OFF Payload Regular Expression
OFF Source /24 Baselines
OFF Protocol Baselines
OFF DNS Malformed
Internet

Arbor-VII


Summary
Name: test22-2
Alert: None
Prefixes: 3.3.3.3/32
Template: Default
TMS Group: TMS4200-TC
Managed Object:
Start Time: 14:57, Jun 22
Stop Time: Ongoing
Edit
Start
Stop
BPS
PPS
Summary
30 Minutes
5 Minutes
1.5 Mpps
1.0 Mpps
500 Kpps
0 pps
17:43
17:44
17:45
17:46
17:47
Pass pps
Drop pps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 422.0 Mbps / 1.1 Mpps | 431.9 Mbps / 1.1 Mpps | 257.1 Mbps / 581.7 Kpps
Passed: 582.9 bps / 0.6 pps | 585.0 bps / 0.6 pps | 52.1 Mbps / 120.2 Kpps
Total: 422.0 Mbps / 1.1 Mpps | 431.9 Mbps / 1.1 Mpps | 309.3 Mbps / 701.9 Kpps
Percent Dropped: 100.00% | 100.00% | 83.15%
Average Blocked Hosts: 0 hosts | 0 hosts | 0 hosts
Countermeasures
Timeframe: 5 minutes
Graph Unit: BPS
Sample Packets
Status
Countermeasure
Dropped
Passed
ON Invalid Packets
OFF Black / White List
ON Zombie Detection
ON TCP SYN Authentication 431.9 Mbps 1.1 Mpps
Enable TCP SYN Authentication
Ignore Source Ports
Example: '22,25'
Ignore Destination Ports
Example: '22,25'
TCP SYN Authentication Idle Timeout
Example: '90' (Leave blank to use default '60')
seconds
Enable HTTP Authentication
HTTP Authentication Ports
Example: '80' (Leave blank to use default '80, 8080')
Save
500 Mbps
0 bps
17:43
17:44
17:45
17:46
17:47
Authenticated due to SYN Authentication: 0 hosts per second
Authenticated due to HTTP Redirect: 0 hosts per second
Authenticated due to proper retransmit behaviour: 0 hosts per second
Total Authenticated: 0 hosts per second
Average Authenticated Hosts: 0.9 hosts
Done
Internet
100%

Cisco guard

- EOS(Satışı yapılmamaktadır)