ISACA
Bilgi sistemlerinde güven ve kalma değer
Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016

Dağıtık Servis Dışı Bırakma Saldırıları (DDOS) ve Harpp DDoS Mitigator

OĞUZ YILMAZ
LABRİS NETWORKS

AJANDA

- Geleneksel Topolojilerde Neden DDoS Başarılı Oluyor?
- Olay İnceleme: Neden Katman 7 inceleme?
- Neden DDoS Yatıştırma ayrı şekilde konumlanmalı?
- HARPP DDOS MITIGATOR Ürün ve Hizmetler
- DDOS Raporu

Temel DDoS Tipleri

Volümetrik Saldırılar (bps)

Saldırı hedefi hedefin giriş bant genişliğini doldurmaktır. (UDP floods, ICMP floods, ve diğer sahte IP sel saldırıları)

Tüketme Saldırıları (pps)

Sunucunun kaynaklarını ya da güvenlik duvarı, yük dengeleme sistemi, IPS gibi ara ekipmanların limitlerini tüketme amaçlıdır. (SYN flood, fragmente paket saldırıları, Ping of Death, Smurf DDoS vb.)

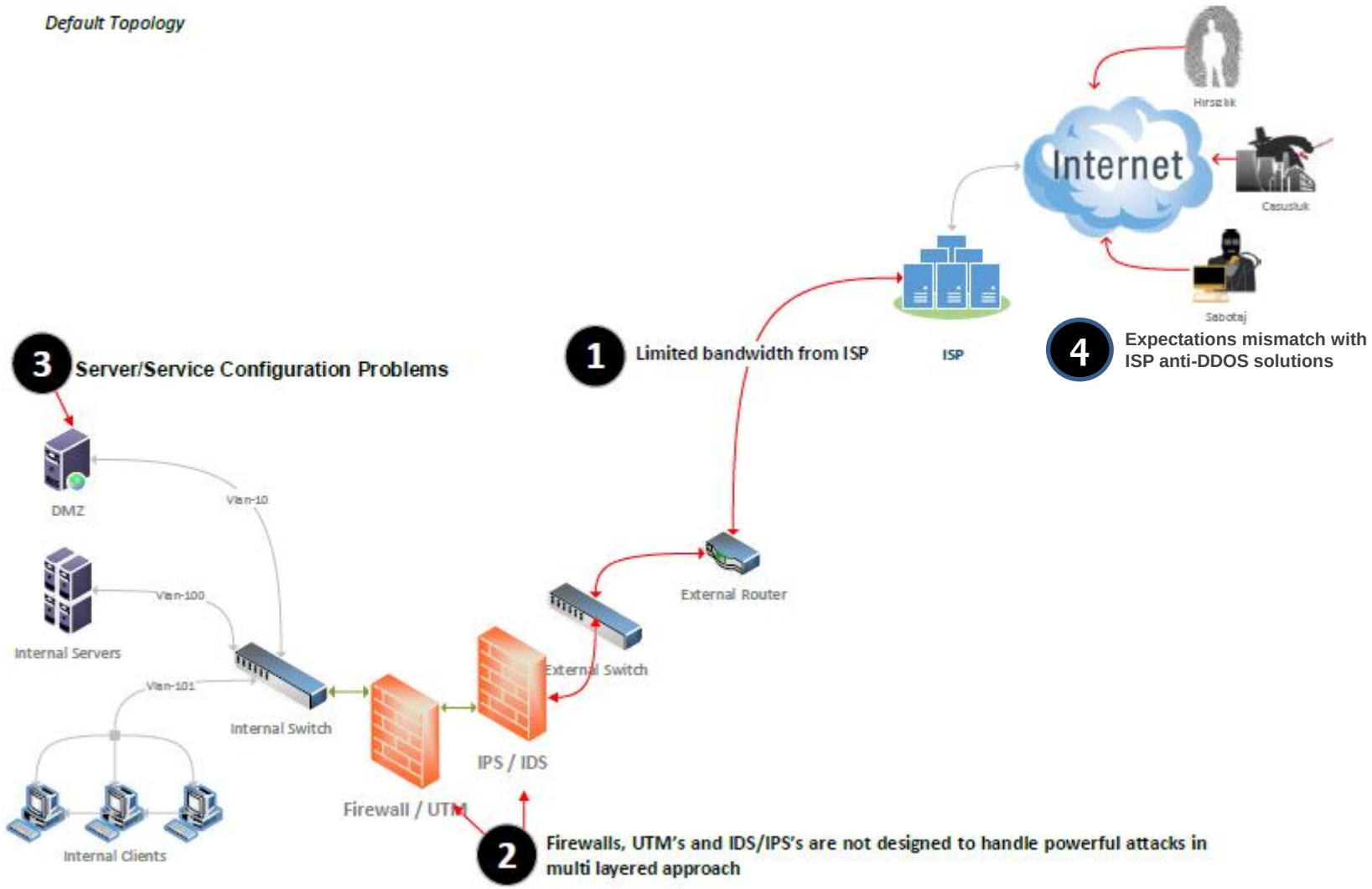
Uygulama Katmanı Saldırıları (req/s)

Katman 7'de gerçekleşen ilgili protokolün komut setini kullanan saldırılardır. (Slowloris, HTTP Flood, SIP Flood, Zero-Day-DoS vb.)

Geleneksel Topolojilerde Neden DDoS Başarılı Oluyor?

HARPP
ddos mitigator

Geleneksel Ağ Topolojisi'nde Sorunlar



Olay İnceleme: Neden Katman 7 inceleme?

Kullanıcı Tipi: E-Ticaret

HARPP
ddos mitigator

Protokol: HTTP (Katman 7)

HTTP 1.0: Her HTTP bağlantısı 1 Katman3 TCP bağlantısı üzerinde.

Günümüzde HTTP artık kaba sığmamaya başladı.

Program ve uygulamaların cihaz üzerinde olmayan, buluttan erişilen veri üzerinden çalışmaları genel yöntem haline geliyor.

Web teknolojileri yüksek interaktivite sağlıyor.

«İste gelsin» değil, «zaten devamlı geliyor». Request/Response değil, Stream.

API'ler buna göre tasarlanıyor.

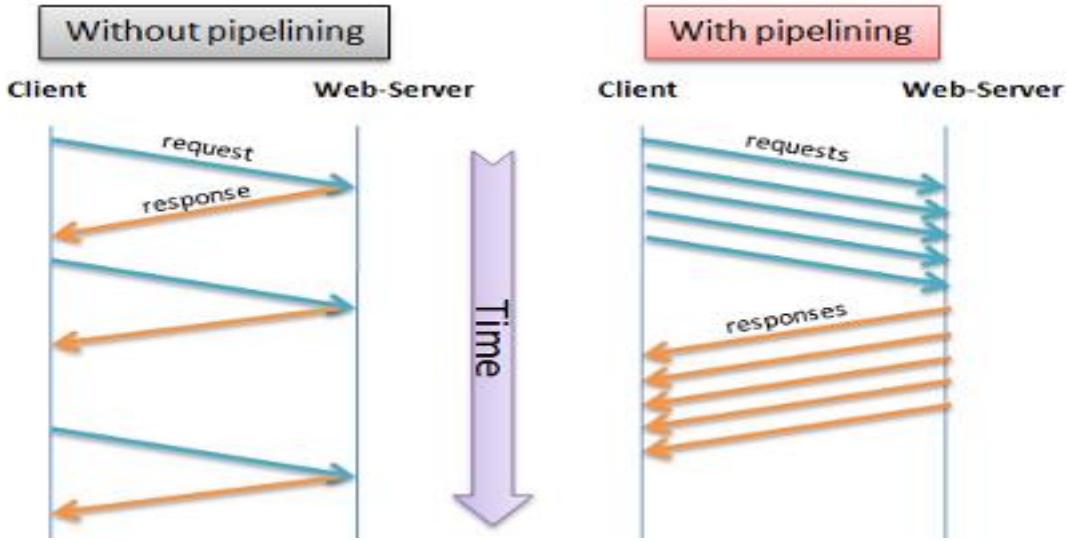
REST & AJAX

Tüm bunlar HTTP ile taşınıyor. Ama her bir HTTP isteği kendi içinde yavaşlığı da getiriyor.

Protokol: HTTP (Katman 7)

HTTP 1.1: Bu nedenle bazı çözümler bulundu ve uygulanıyor.

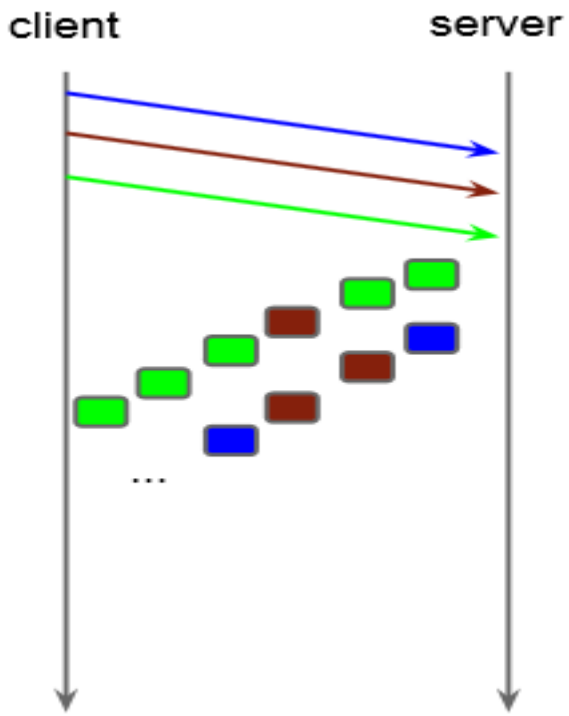
Pipelining



Artık HTTP için L3'te bakılınca çok bağlantı görmek zorunda değiliz.

Protokol: HTTP (Katman 7)

SPDY & HTTP/2



Multiplexed stream
Stream önceliklendirme
Stateful HTTP başlık sıkıştırma

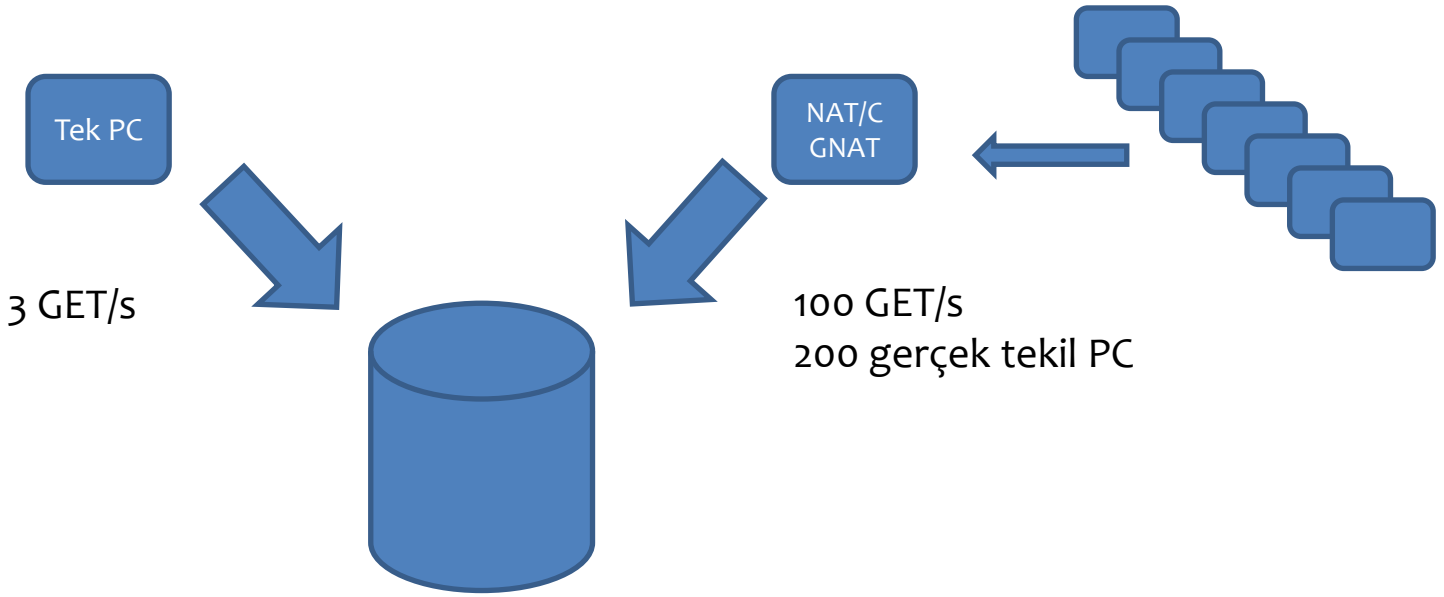
L3'teki yansıma tamamen farklı.

1 L3 TCP bağlantı

QUIC?

Protokol: HTTP (Katman 7)

NAT edilmiş ve edilmemiş trafiğin birlikte geldiği düşünüldüğünde de eşik değeri bazlı L3 yöntemleri ve hatta eşik değeri bazlı L7 yöntemleri büyük sorunlara gebedir.



Protokol: HTTP (Katman 7)

Detaylı inceleme de aldatıcı olabilir.

/index.php?id=4348583
/index.php?id=1249584
/index.php?id=6747637
/index.php?id=2874656
/index.php?id=5657576
/index.php?id=0954767

Bu şekilde bir istek, akılsız bir detaylı inceleme motorunda farklı istekler gibi algılanabilir. Halbuki URL değiştirerek atlatma kullanan bir saldırı tekniğidir.

DDI: Deep DDoS Inspection

DDI™ Katman 7'de çalışır.

- Yapay Zeka/Makine Öğrenmesi
- NAT, Tek PC ayrımı
- Protokol uygunluk kontrolü
- URL farklılık kontrolü
- URL ve HTTP başlıklarında Robot algılama
- Bilinen saldırı araçlarının tanınması
- POST içerik kontrolleri ile aldatma koruması
- Protokol özel içerik kontrolü

Neden DDoS Yatıştırma ayrık şekilde konumlanmalı?

Smokescreening / Sisleme

DDoS daha zeki saldırıları gizlemek için kullanılıyor.

1. Mekanizma: Odak Şaşırtma

2. Mekanizma: İzleme ve İnceleme kapasitesinin aşımı

Bu mekanizmada gerçek kurban sunucu değil;

a- Saldırı Tespit ve Önleme Sistemleri (IPS)

b- SIEM

c- Malware Engelleme Sistemleri,

gibi yüksek maliyetli sistemlerdir.

Odak Şaşırtma

Örnekler:

«Dirt Jumper» DDoS saldırıları, 2013.

Yasadışı transferler sonrası DDoS saldırıları

Fraud işlemleri sırasında DDoS saldırıları

DDoS hedefi olan kurumların %55'i aynı zamanda veri çaldırma, para çaldırma ya da kötücül yazılım çalıştırma mağduru *

* Neustar 2015 EMEA DDOS report

İzleme ve İnceleme kapasitesinin aşımı

Örnekler:

2013: BIPS Bitcoin: 1M USD Bitcoin bir DDoS saldırısı sırasında çalındı.

2015: Carphone Warehouse Veri Sızıntısı: 2.4 milyon müşteri bilgisi DDoS sırasında çalındı.

Labris SOC ve HARPP CERT İstatistikleri

Aynı Zamanda Portscan ve Zayıflık Tetikleme	1 gün	28%
	1 hafta	70%
Aynı Zamanda DDoS ve Zayıflık Tetikleme	1 gün	6%
	1 hafta	21%

Tüm DDoS'lar içinde Karma-DDoS	18%

IPS Kurban: Laboratuvar Simülasyonu

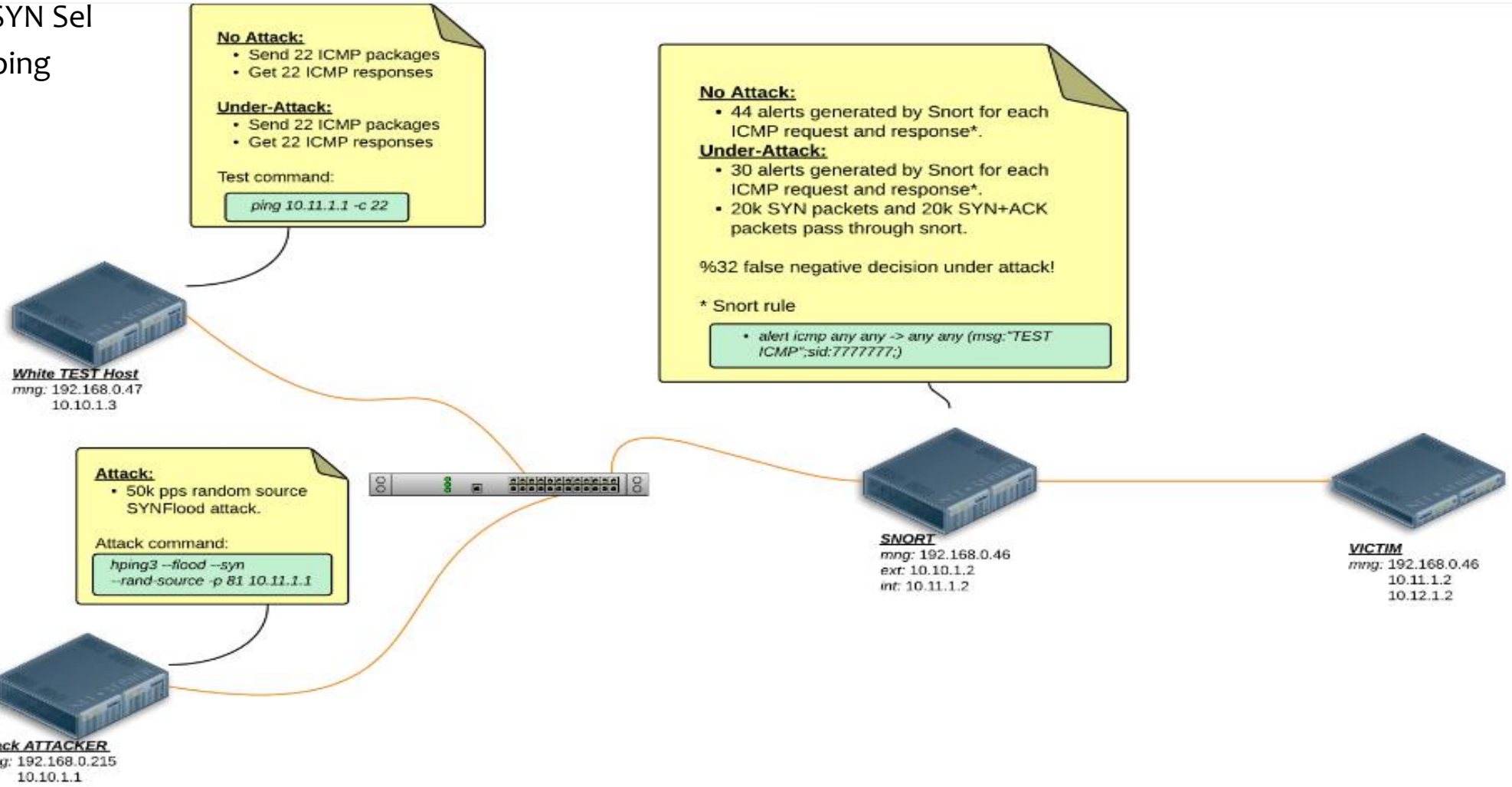
Siber Savaş Laboratuvarımızda (CWL) benzer senaryoyu simüle ettik. Sonuçlar benzer.

Açık Kaynak Snort IPS motoru (IPS'lerin 1/3 ündeki ana motor)

Simülasyon 1:

Saldırı: L3 TCP SYN Sel

Kontrol: ICMP ping

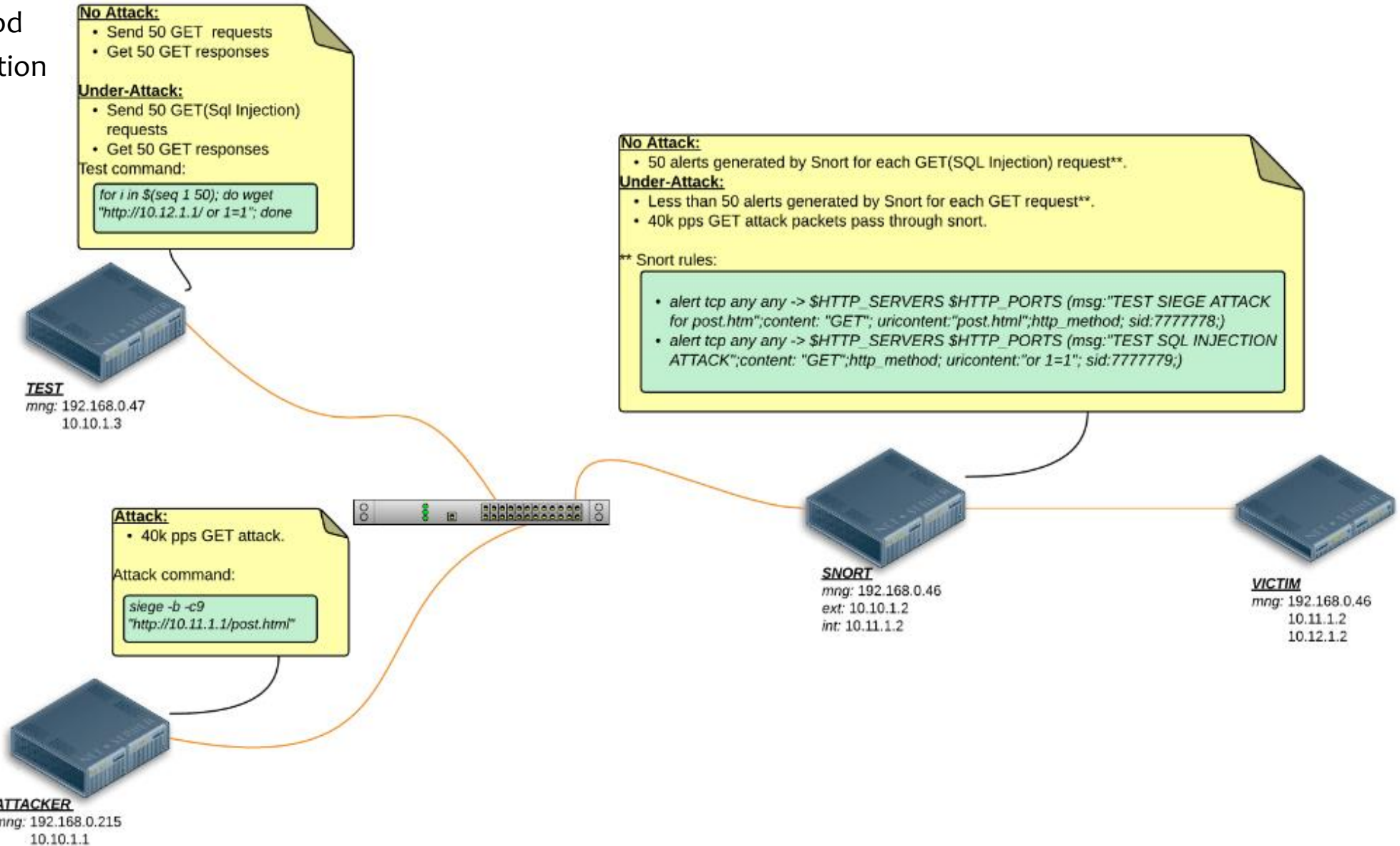


IPS Kurban: Laboratuvar Simülasyonu

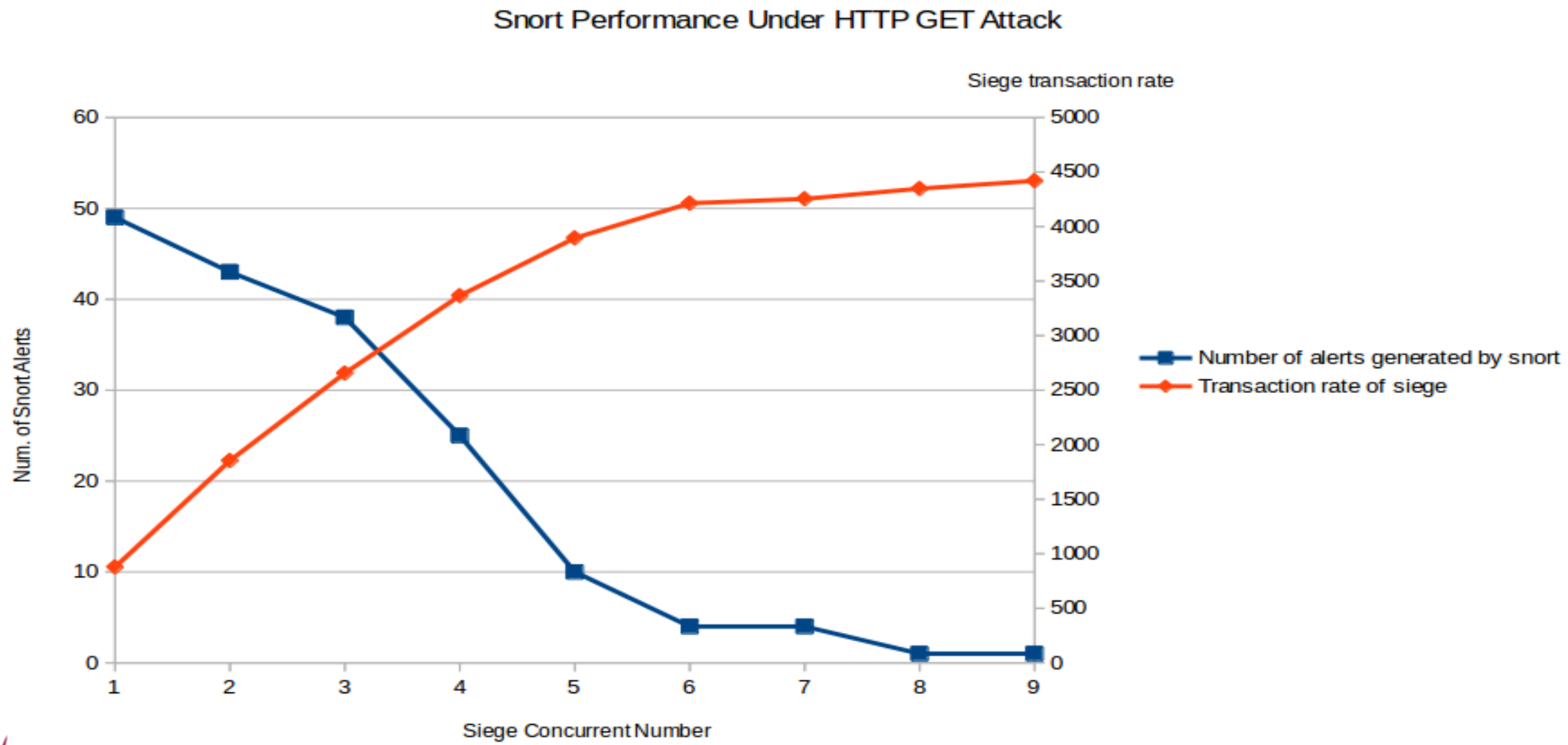
Simülasyon 2:

Saldırı : L7 GET Flood

Kontrol : SQL Injection



IPS Kurban: Laboratuvar Simülasyonu



IPS Kurban: Laboratuvar Simülasyonu

- IPS'lerdeki Darboğazlar:
  - İnceleme kapasitesi
  - Ağ kapasitesi
  - Gecikme
  - Saniyedeki bağlantı
  - Aynı andaki oturum

- Neden etkilendi?
  - Ethernet'ten paket alımı
    - Interrupts, queues, buffers
  - SYN koruma mekanizmaları
  - Paket birleştirme, açma ve inceleme
    - L7 payload inceleme
  - Kötü multi-thread verimi
  - Kayıt tutma ve Raporlama fonksiyonları
  - Diğer 1.000 'lerce imza

Öneriler

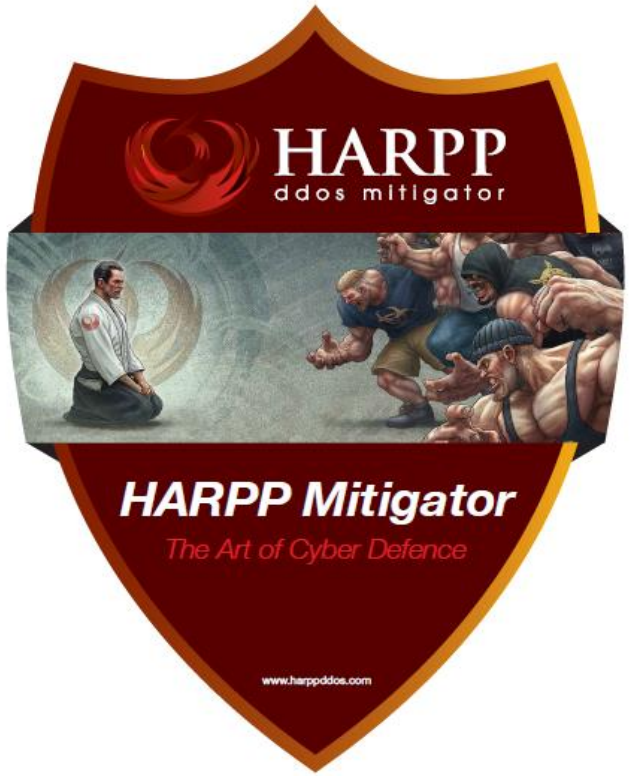
DDOS Sisleme konvansiyonel L7 güvenlik önlemlerini geçmek için gittikçe popülerleşiyor.

Aksiyonlar:

1- İşe özel ve tüm diğer ürünlerin önünde Anti-DDOS CPE (Hibrit koruma)
2- ISP DDoS Koruma servisleri ile bant genişliği koruması
3- Takım tepki planı, DDoS sorumlusu
4- DDoS sırasında DDoS dışı saldırıları için daha da tetikte olunması
5- DDoS özel CERT takımlarının olaya müdahale ve alan bilgisi (aynı saat içinde yatıştırma)

HARPP DDOS MITIGATOR
Ürün ve Hizmetler

HARPP
ddos mitigator



Guard of the Guards

«Quis custodiet ipsos custodes»

DDOS CERT

Computer Emergency Response Team

DDOS Yatıştırma Cihazları

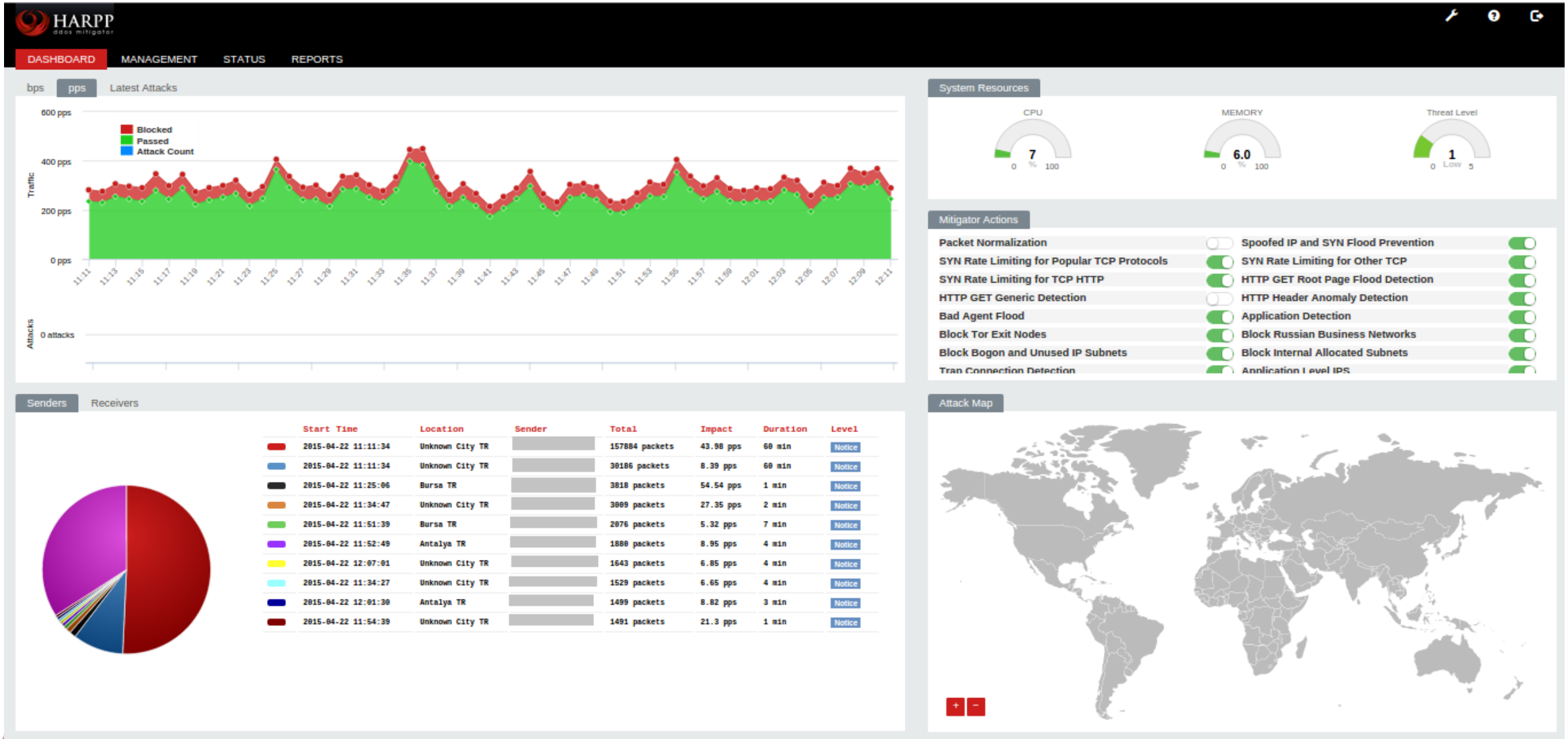
Olaya Müdahale Hizmetleri (CERT)

Uygulama Koruma - HARPP DDOS Mitigator

Guard of the Guards:
Tüm DoS/DDoS savunma tekniklerini bir arada toplayan tek çözüm

- DDoS Özel Yüksek Performanslı Donanım
- Dinamik Anormallik Tespiti (DDI)
- L7 Özel DoS/DDoS IPS
- Çoklu Protokol Destekli
- Web Yönetimi
- Delil toplama ve zaman damgalama

HARPP DDoS Mitigator Dashboard



ISACA
Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016, İSTANBUL

Rekabet Analizi ve DDI™ Teknolojisi

Bazıları yalnızca OSI L4 odaklıdır.	Harpp ise OSI L7 ‘ye odaklanır. (DDI™)
Statik eşik değer bazlı tasarlanmıştır.	Harpp ise Makine Öğrenmesi ve AI bazlıdır.
Pahalıdır. Özel ASIC ve pahalı donanım mimarilerinde çalışırlar.	Harpp kolay ulaşılır, x86 donanımlar üzerinde çalışır. Donanım bağımlı değildir. Bulut çözümlere açıktır.
Bazıları HTTP gibi tek protokole yoğunlaşır.	Harpp Çoklu-Protokol ürünü olarak tasarlanmıştır.
Bazıları geç tepki verir.	Harpp ise gerçek zamanlıya yakın çalışır.
Bazı çözümler, bypass edilebilir trafik yönlendirme bazlıdır.	Harpp ağa girer. Bypass mümkün değildir.
Diğer çözümler ya cihaz ya hizmettir.	Harpp donanımı ve üreticiden olaya müdahale hizmetini bir arada sunar.

Servis Koruma: Benzersiz CERT ve SOC

Harpp Olaya Müdahale ekibi hazırdır!

İzleme

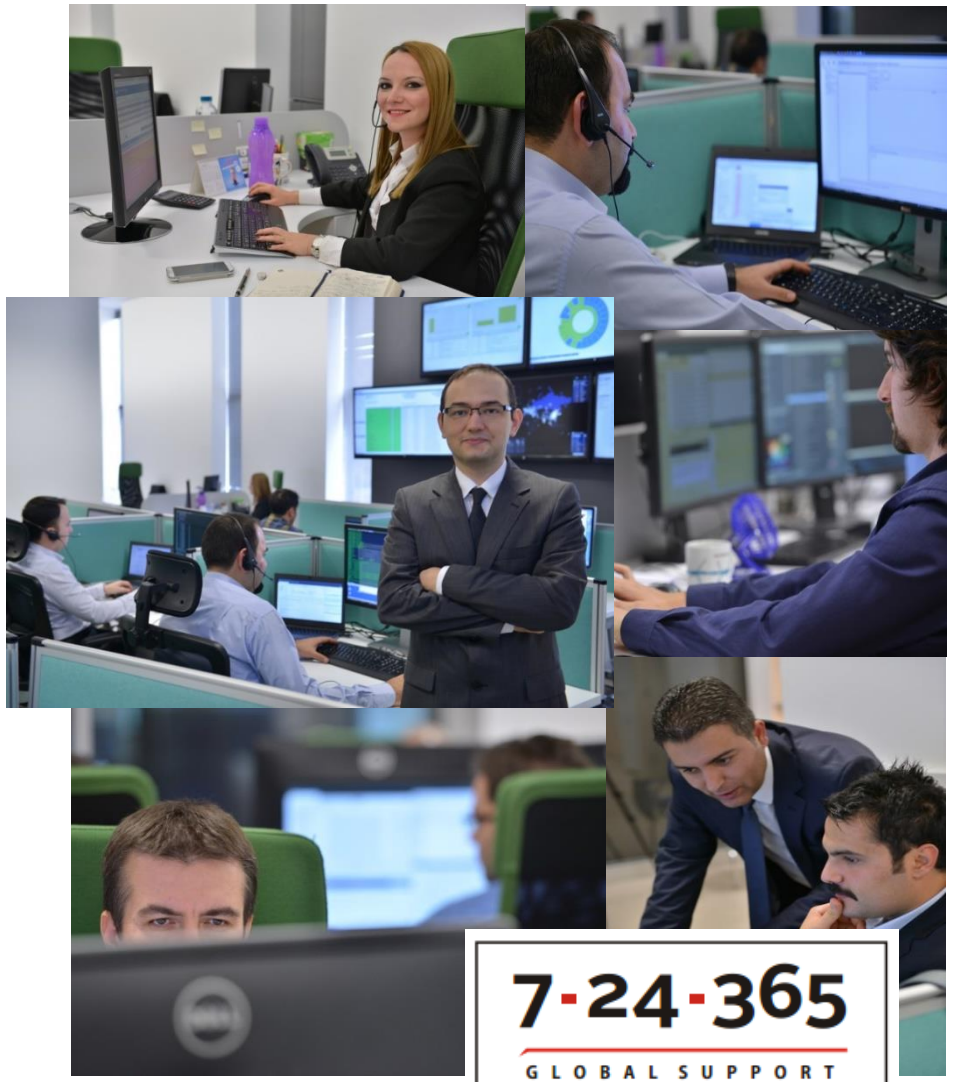
Olaya Müdahale

Raporlama

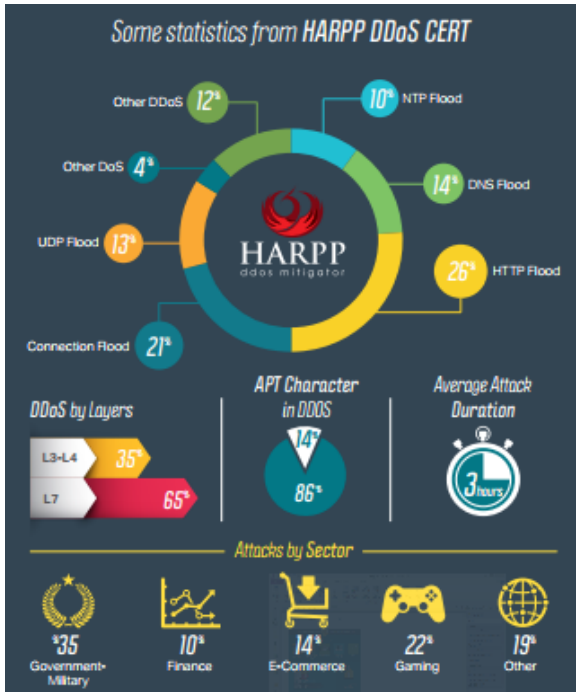
7-24-365

GLOBAL SUPPORT

Servis Koruma: Benzersiz CERT ve SOC



DDOS CERT
Computer Emergency Response Team
CWL
cyber warfare lab

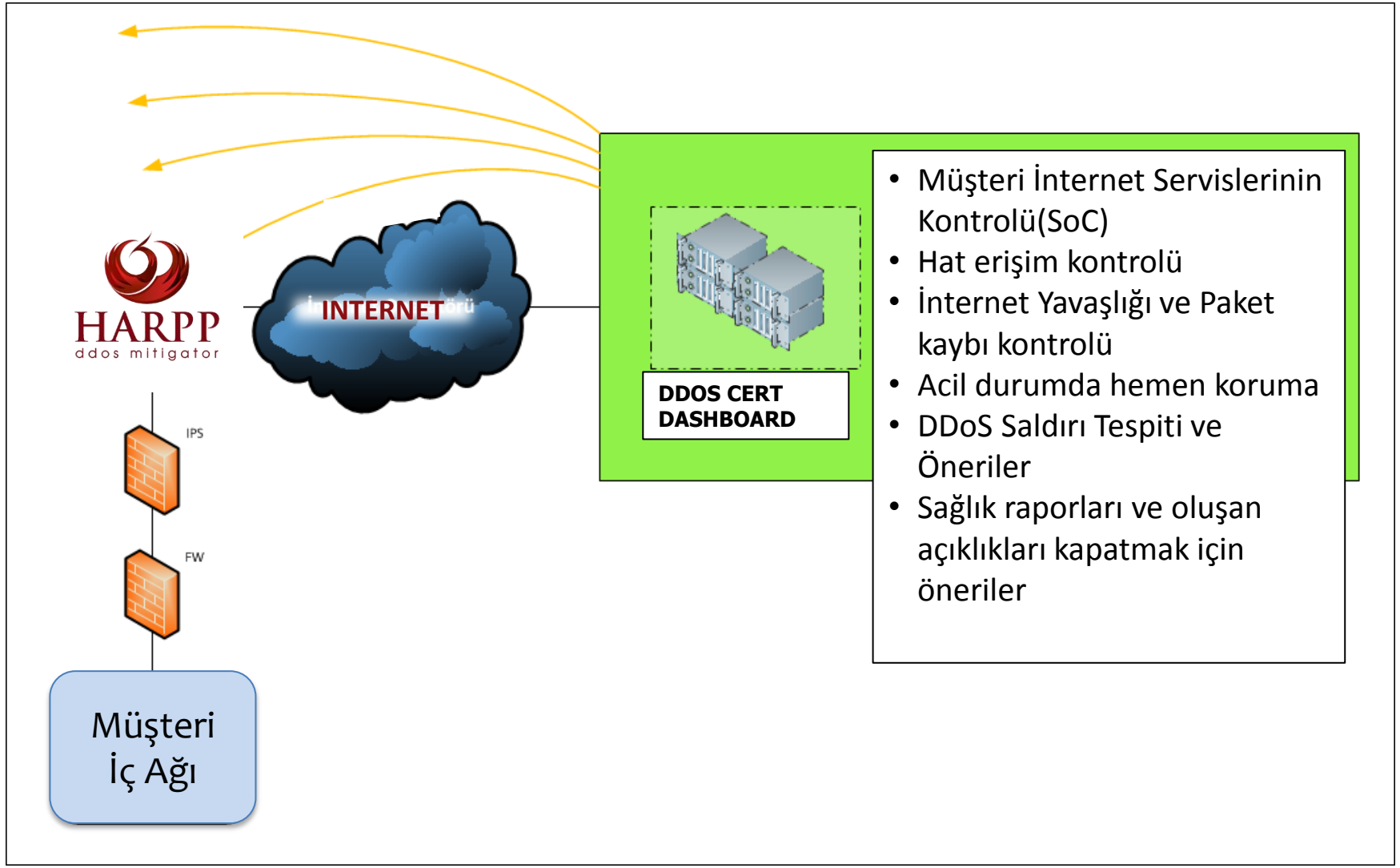


ISACA®
Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

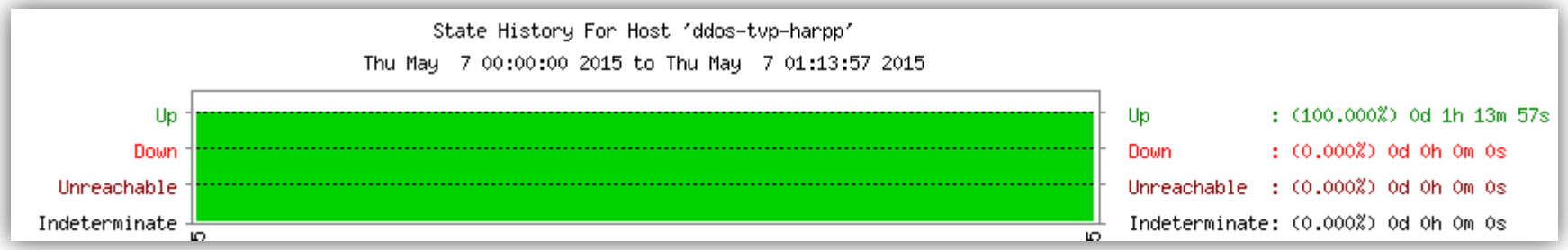
3-4 MART 2016, İSTANBUL

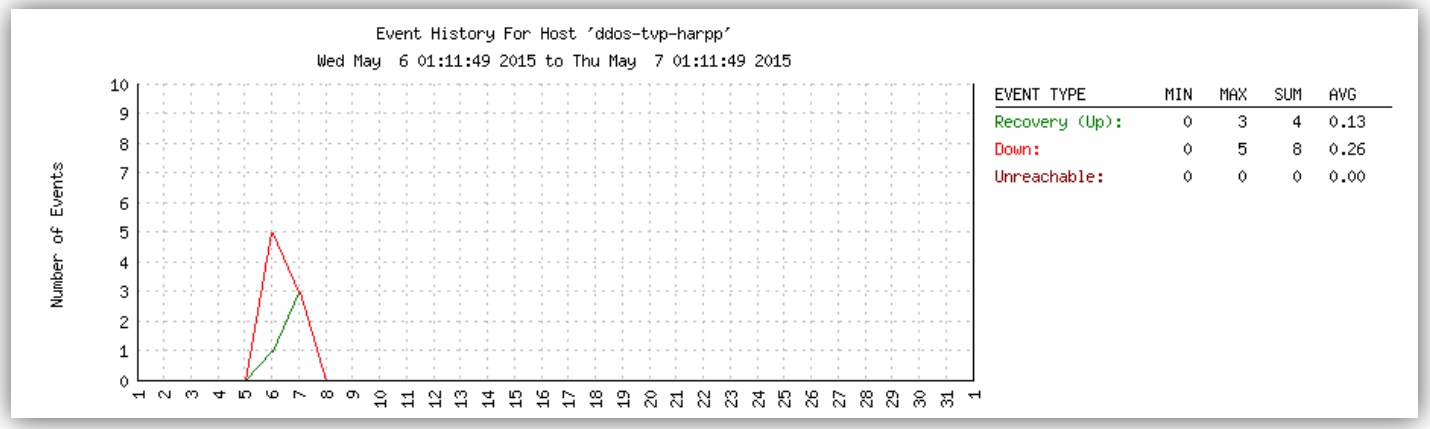
HARPP DDoS CERT İzleme



HARPP DDoS CERT 7x24 İzleme

Host	Service	Status	Last Check	Duration	Attempt
ddos-tvp-harpp	check_ssh	OK	05-07-2015 01:05:33	0d 11h 38m 48s	1/3
ddos-tvp-mon	check_http	OK	05-07-2015 01:08:29	0d 0h 10m 38s	1/3





ISACA Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016, İSTANBUL

HARPP DDoS CERT Hizmet Akışı

1 –Demo Süreci

- Sunum
- Uzaktan Demo
- Cihaz ile Demo
- Kısa PoC
- Detaylı PoC

2 – Aktivasyon & Kurulum

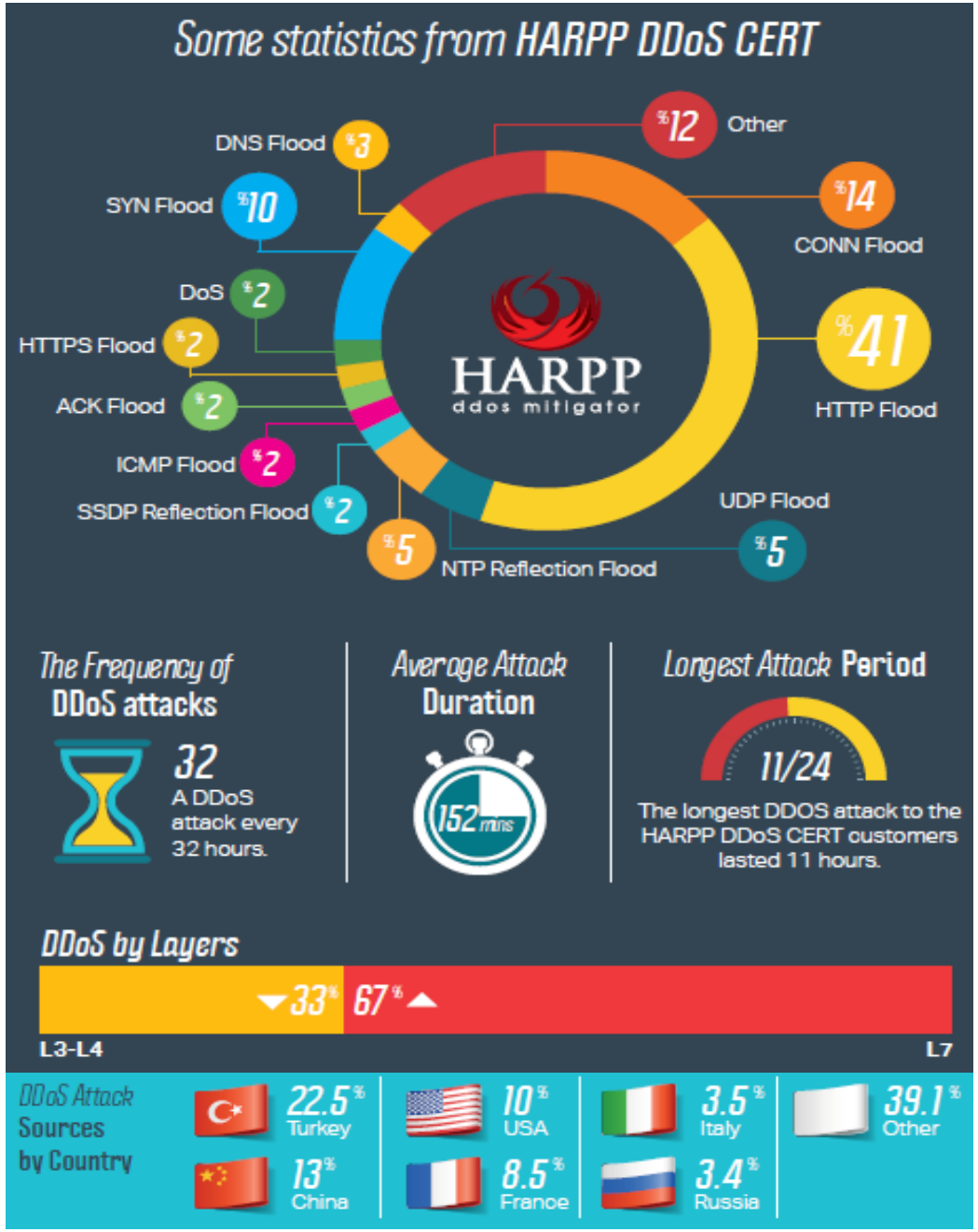
- ❑ Aktivasyon Toplantısı
- ❑ Topoloji Tasarımı
- ❑ Teknik Gereksinim Formu
- ❑ Aktivasyon Planı ve Onayı
- ❑ Aktivasyon Ayarları

3 – Sürekli

- İzleme (NMS, Alarm Takibi) *
- Sağlık Raporları *
- Sistem İyileştirme Raporları *

4 – Saldırıdan Sonra

- ❑ DDoS Saldırı Sonrası Raporu
- ❑ Sistem Sağlık Raporu



http://labrisnetworks.com/labris-soc-annual-report/

HARPP
ddos mitigator

@harpp_ddos /labristeknoloji @LabrisTeknoloji /Labrismedya

www.labrisnetworks.com - www.harppddos.com