Samuel Bonete
S.Engineer Fortinet
sbonete@fortinet.com

FORTINET®

Seguridad en e-Administración

Seguridad en e-Administración

Portales Web

- 49% de las web apps tienen vulnerabilidades de alto riesgo susceptibles de ser explotadas con herramientas automáticas.
- 80%-96% son vulnerables a ataques manuales
- 99% no cumplen el estándar PCI DSS
- La mayoría de las vulnerabilidades no son resueltas por las tecnologías firewall tradicionales
  - Cross-site scripting
  - SQL injection
  - Information Leakage
  - HTTP Response Splitting

Cuentas Usuarios

VPN - SSL
eMail Corporativo
App Web Cloud
etc

Denegación de Servicio

Portales Web

- 49% de las web apps tienen vulnerabilidades de alto riesgo susceptibles de ser explotadas con herramientas automáticas.
- 80%-96% son vulnerables a ataques manuales
- 99% no cumplen el estándar PCI DSS
- La mayoría de las vulnerabilidades no son resueltas por las tecnologías firewall tradicionales
  - Cross-site scripting
  - SQL injection
  - Information Leakage
  - HTTP Response Splitting

b

les
las

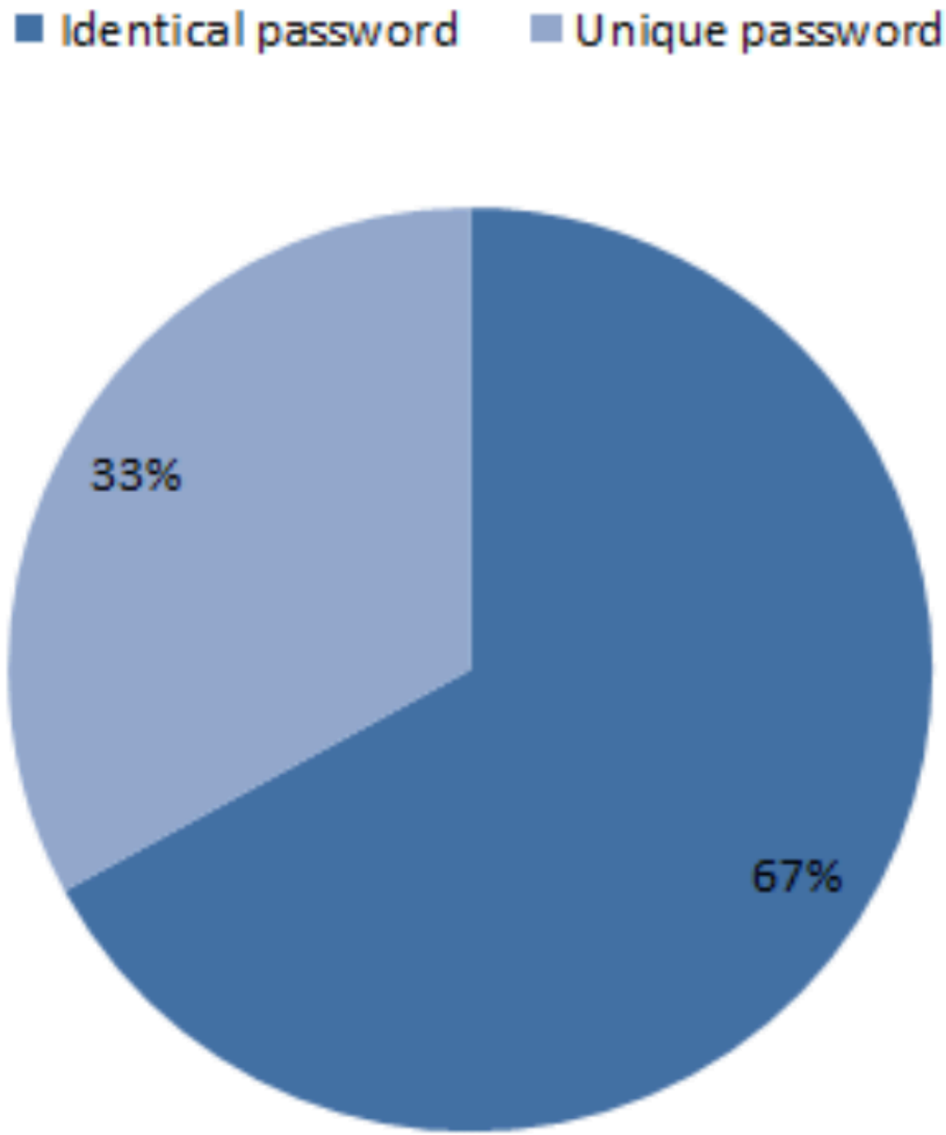
ales

Cuentas Usuarios

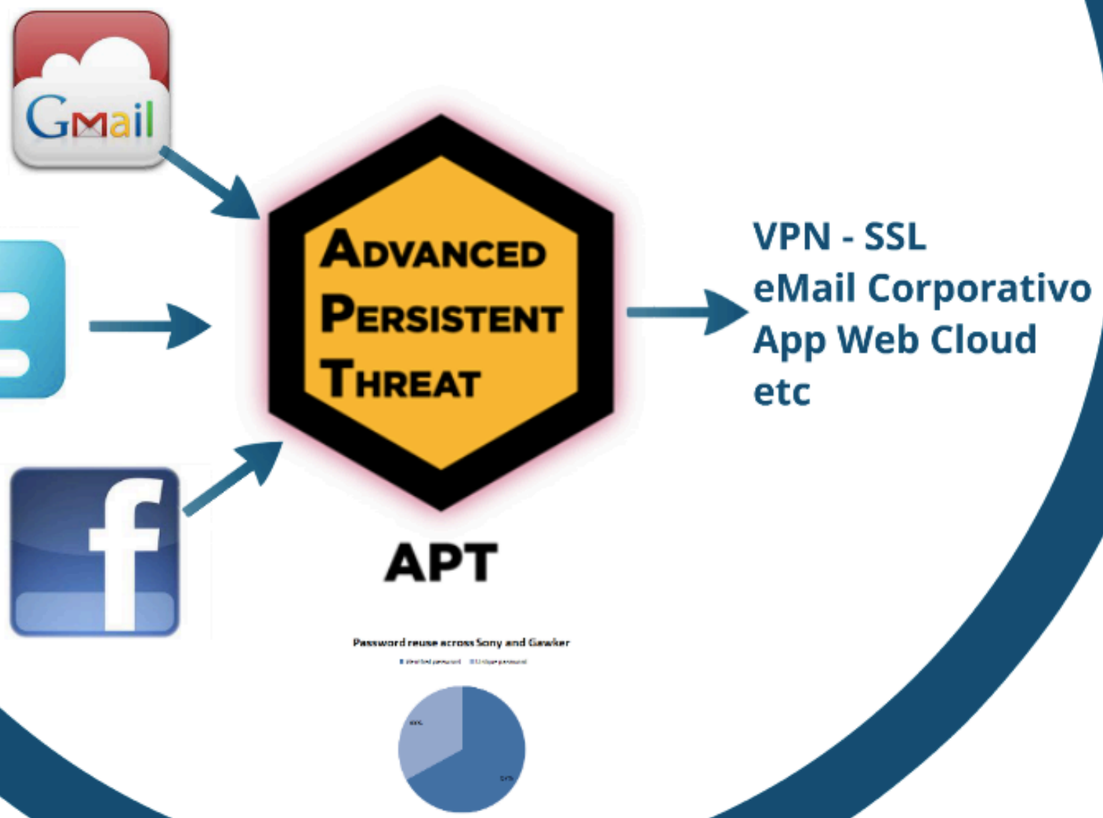
VPN - SSL
eMail Corporativo
App Web Cloud
etc

APT

Password reuse across Sony and Gawker



Cuentas Usuarios



Denegación de Servicio

SL
orporativo
b Cloud

sbonete@fortinet.com

FORTINET

Seguridad en e-Administración

Portales Web

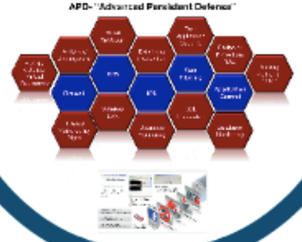
- 49% de las web apps tienen vulnerabilidades de alto riesgo susceptibles de ser explotadas con herramientas automáticas.
- 80%-96% son vulnerables a ataques manuales
- 99% no cumplen el estándar PCI DSS
- La mayoría de las vulnerabilidades no son resueltas por las tecnologías firewall tradicionales
  - Cross-site scripting
  - SQL injection
  - Information Leakage
  - HTTP Response Splitting

Cuentas Usuarios

Denegación de Servicio

FortiWEB

Multiples capas



Anti-DDoS

FortiWEB

Escaner de vulnerabilidades Web
Escanea, analiza y detecta vulnerabilidades de aplicaciones Web

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

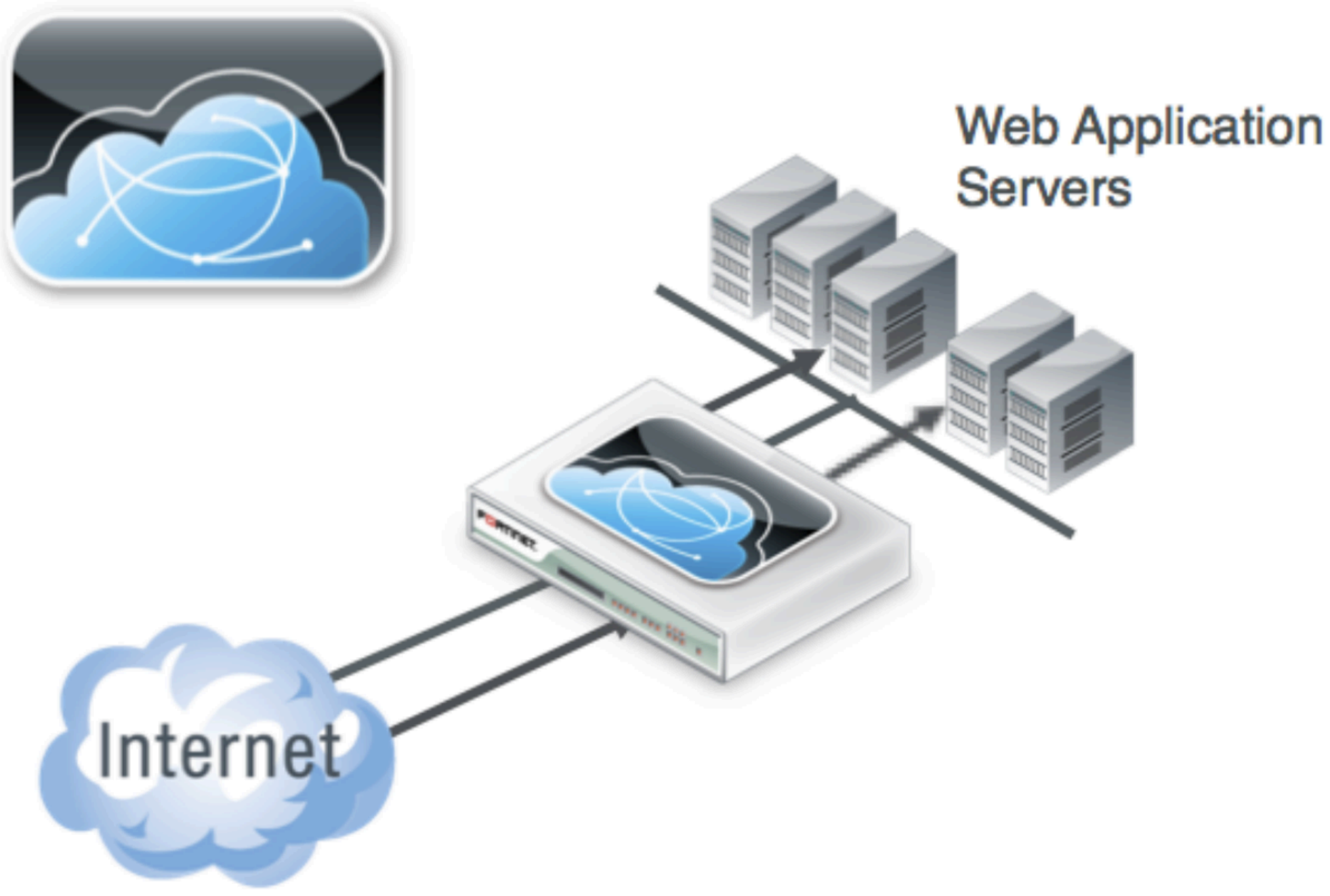
Firewall de aplicaciones Web - WAF
Securiza apps Web protegiendo frente a ataques y ayudando al cumplimiento regulatorio

Application delivery
Garantiza la disponibilidad y asegura el rendimiento de las aplicaciones Web críticas

DDoS Http
Protección contra ataques de DDoS a servicios web

Securiza aplicaciones Web | **Protege Web Services** | **Optimiza la entrega de Aplicaciones**

FortiWeb



Escaner de vulnerabilidades Web

Escanea, analiza y detecta vulnerabilidades de aplicaciones Web

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

Firewall de aplicaciones Web - WAF

Securiza apps Web protegiendo frente a ataques y ayudando al cumplimiento regulatorio

Application delivery

Garantiza la disponibilidad y asegura el rendimiento de las aplicaciones Web críticas

DDoS Http

Protección contra ataques de DDoS a servicios web

Securiza aplicaciones Web

Protege Web Services

Optimiza la entrega de Aplicaciones

FortiWEB

Escaner de vulnerabilidades Web
Escanea, analiza y detecta vulnerabilidades de aplicaciones Web

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

Firewall de aplicaciones Web - WAF
Securiza apps Web protegiendo frente a ataques y ayudando al cumplimiento regulatorio

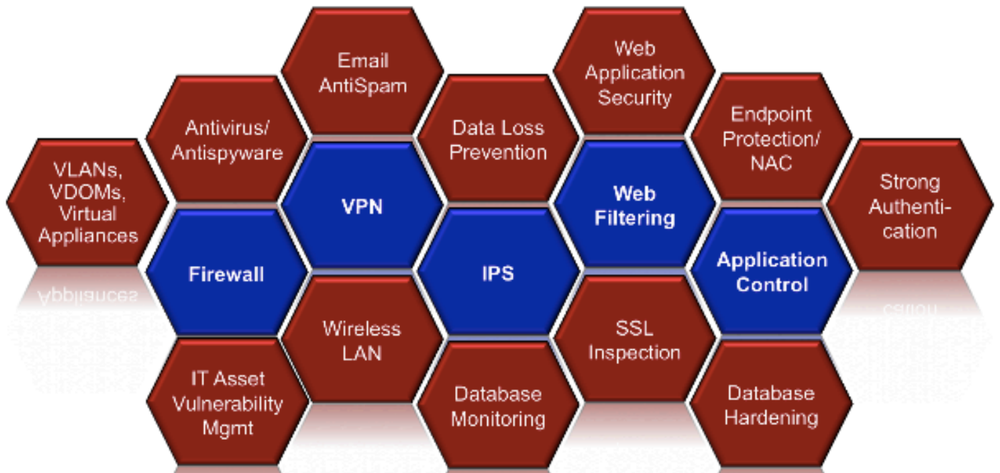
Application delivery
Garantiza la disponibilidad y asegura el rendimiento de las aplicaciones Web críticas

DDoS Http
Protección contra ataques de DDoS a servicios web

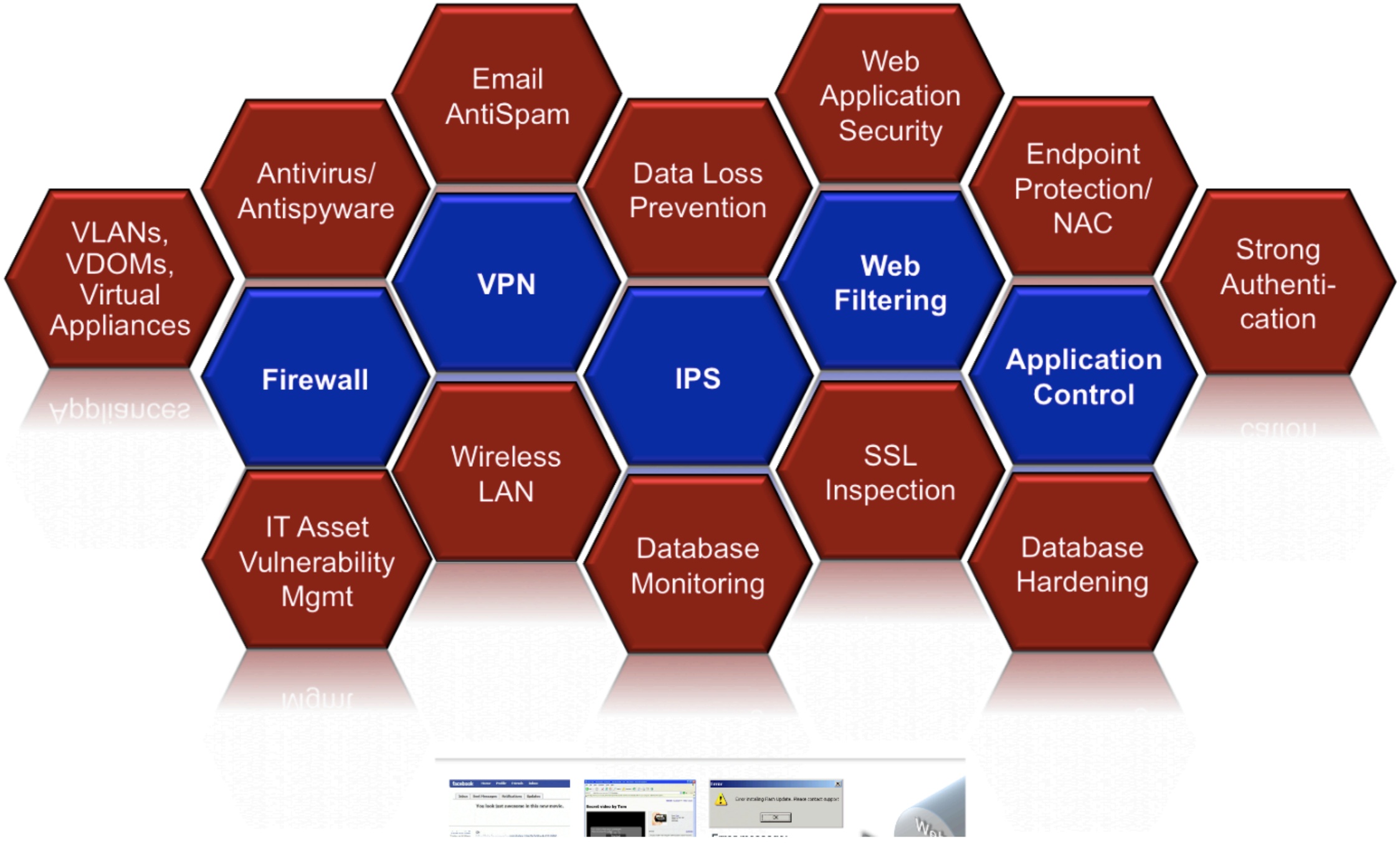
Securiza aplicaciones Web | **Protege Web Services** | **Optimiza la entrega de Aplicaciones**

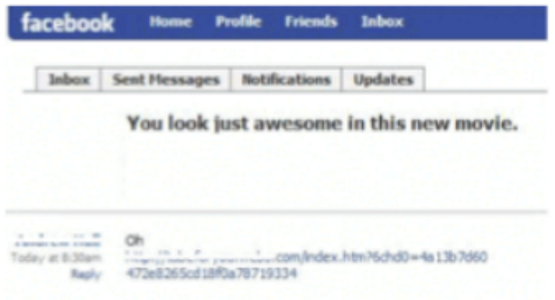
Multiples capas

APD- “Advanced Persistent Defense”

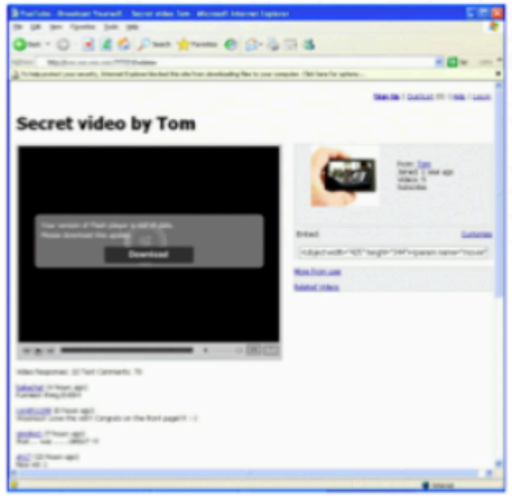


APD- “Advanced Persistent Defense”

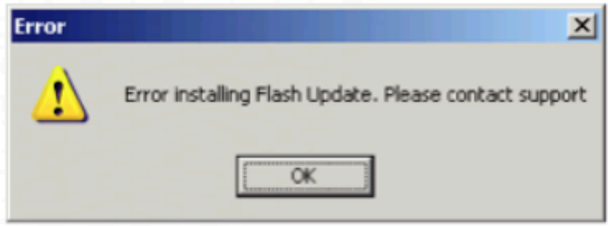




“Innocent” Video Link:
»Redirects to malicious Website



“Out of date” Flash player
»Download malware file



Error message:
»Installs on system and attempts to propagate

Integrated Web Filtering
Blocks access to malicious Website

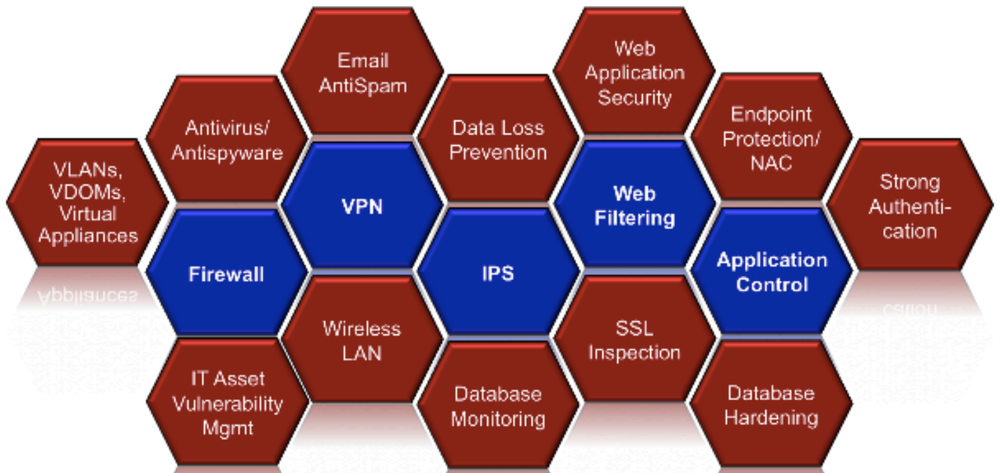
Network Antivirus
Blocks download of virus

Intrusion Prevention
Blocks the spread of the worm

Authentication & Encryption

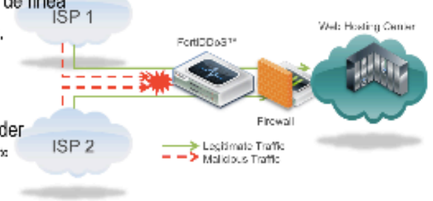
Multiples capas

APD- “Advanced Persistent Defense”



Anti-DDoS

- Utiliza el último miembro de la familia de FortiASIC,, FortiASIC-TP[TM]
- Detección a velocidad de línea
- En línea, transparente.
  - Sin cambios de MAC
- No basado en firmas
  - Basado en patrones
- Preparado para aprender
  - Se adapta según comportamiento
- Protección granular
  - Múltiples umbrales proporcionan múltiples protecciones



Servicio de limpieza del ISP o proveedor de en la nube.

Modelo: Servicio gestionado de subs-cripción. Normalmente separada la mitigación de la detección. P

Pros: Despliegue rápido, firma contrato.

Cons: Caro, inflexible y costes variables dependiendo de los ataques. Poca parametri-zación.

Firewall / IPS

Modelo: Integrado en el dispositivo FW/IPS del cliente.

Pros: Dispositivo único, arquitectura simplificada.

Cons: No tiene un diseño específico para detectar y detener bots o ataques DDOS complejos.

Dispositivo Dedicado

Modelo: Detección, mitigación y reporting en línea con el tráfico. Auto detección de un amplio abanico de ataques DDOS

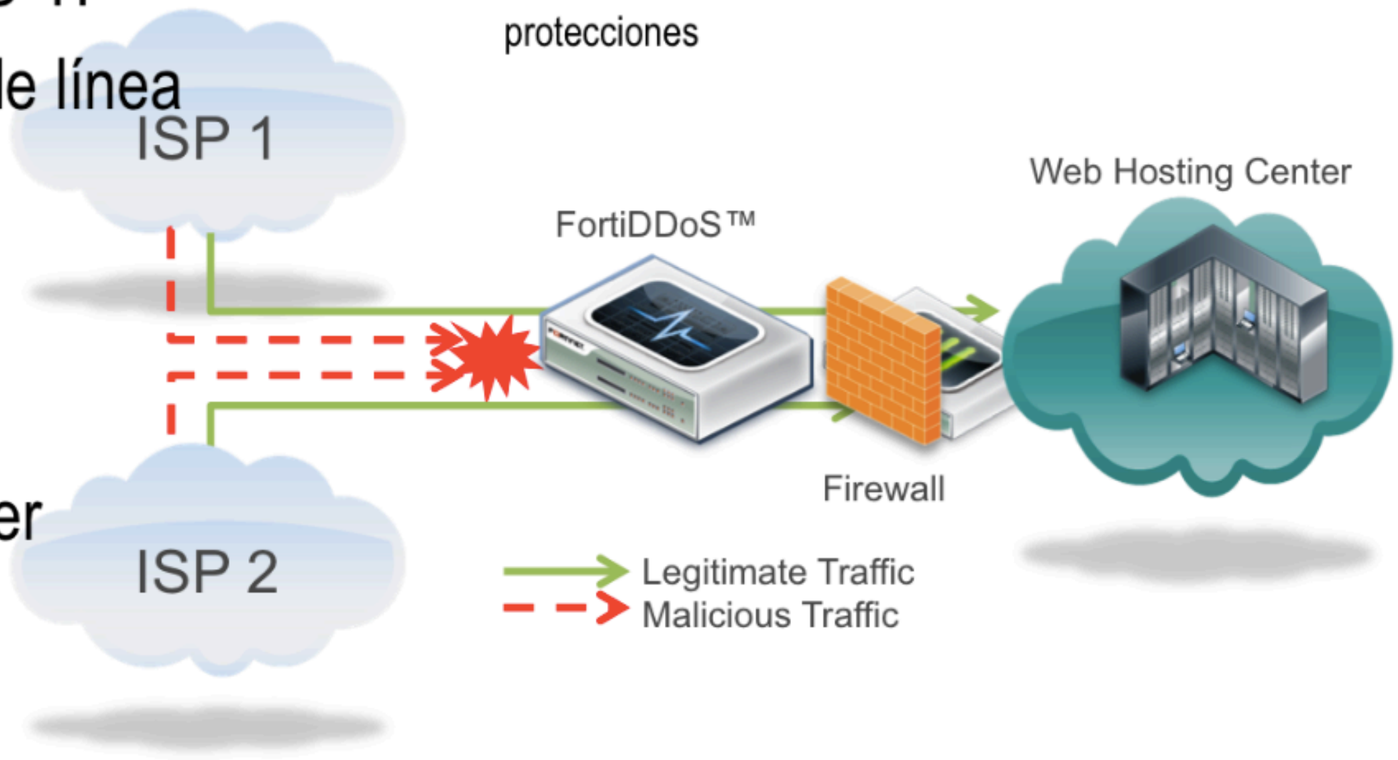
Pros: Costes controlados, sin sorpresas. Multicapa, rápido y sencillo de desplegar.

Cons: Un elemento adicional de red.

Defensa AntiDDOS con aceleración HW

Protection basada en Intención

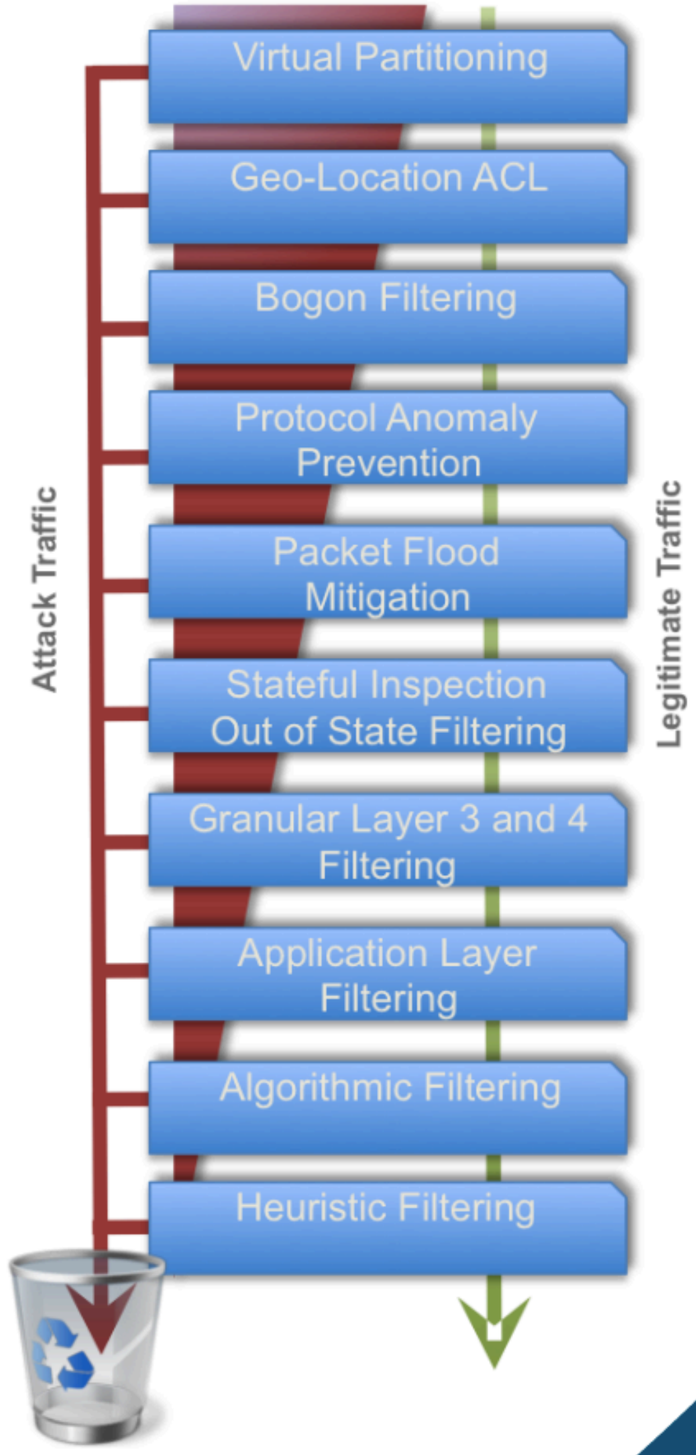
- Utiliza el último miembro de la familia de FortiASIC,, FortiASIC-TP™
- Detección a velocidad de línea
- En línea, transparente.
  - Sin cambios de MAC
- No basado en firmas
  - Basado en patrones
- Preparado para aprender
  - Se adapta según comportamiento
- Protección granular
  - Múltiples umbrales proporcionan múltiples protecciones



n HW

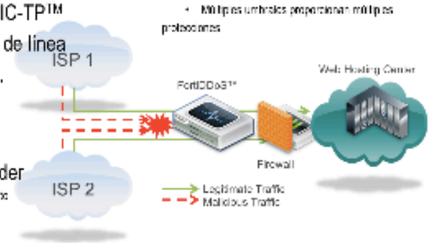
ción granular

es umbrales proporcionan múltiples



Anti-DDoS

- Utiliza el último miembro de la familia de FortiASIC,, FortiASIC-TP[IM]
- Detección a velocidad de línea
- En línea, transparente.
  - Sin cambios de MAC
- No basado en firmas
  - Basado en patrones
- Preparado para aprender
  - Se adapta según comportamiento
- Protección granular
  - Múltiples umbrales proporcionan múltiples protecciones



sbonete@fortinet.com

FORTINET

Seguridad en e-Administración

Portales Web

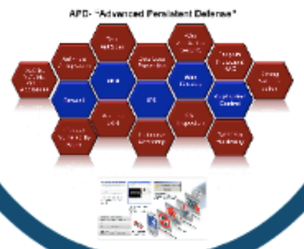
- 49% de las web apps tienen vulnerabilidades de alto riesgo susceptibles de ser explotadas con herramientas automáticas.
- 80%-96% son vulnerables a ataques manuales
- 99% no cumplen el estándar PCI DSS
- La mayoría de las vulnerabilidades no son resueltas por las tecnologías firewall tradicionales
  - Cross-site scripting
  - SQL injection
  - Information Leakage
  - HTTP Response Splitting

Cuentas Usuarios

Denegación de Servicio

FortiWEB

Multiples capas



Anti-DDoS

Muchas gracias

Samuel Bonete
S.Engineer Fortinet
sbonete@fortinet.com