

# Mario Arriaza - Fundador



El Salvador



Guatemala



Honduras



Nicaragua



Panamá



Costa Rica

## Grupo Intelector – Fundado en 1998

Compañía Regional con operaciones en El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica y Panamá.





### Servicio de seguridad

### Indicaciones



GUARDAR



## EN ALREDEDORES



[ENVIAR AL TELÉFONO](#)



COMPARTIR



San José



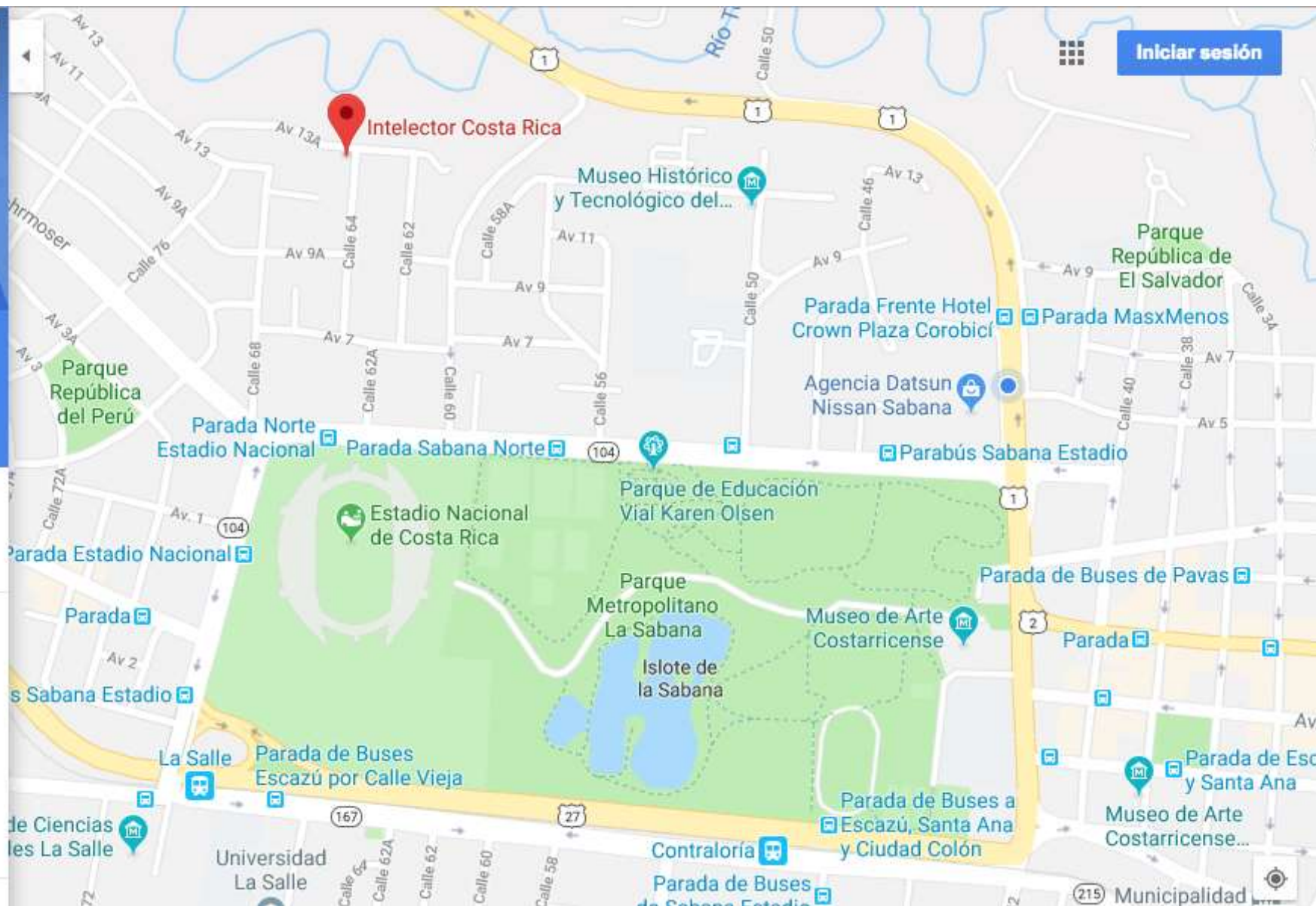
grupointelector.com



4034 3129

[Reclamar esta empresa](#)

[SUGERIR UNA EDICIÓN](#)



## Cientes – Sector Financiero



**BDF**



*Banco ProCredit*





## Cientes – Sector Industria



# Estrategias de Mitigación para Ataques DDoS

Ing. Mario Arriaza



## LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS



### Técnicas de Denegación de Servicio

**Art. 14.-** El que de manera intencionada, utilizando las técnicas de la denegación de servicio o prácticas equivalentes que afectaren a los usuarios que tienen pertenencia en el sistema o red afectada, imposibilite obtener el servicio, será sancionado con prisión de tres a cinco años.



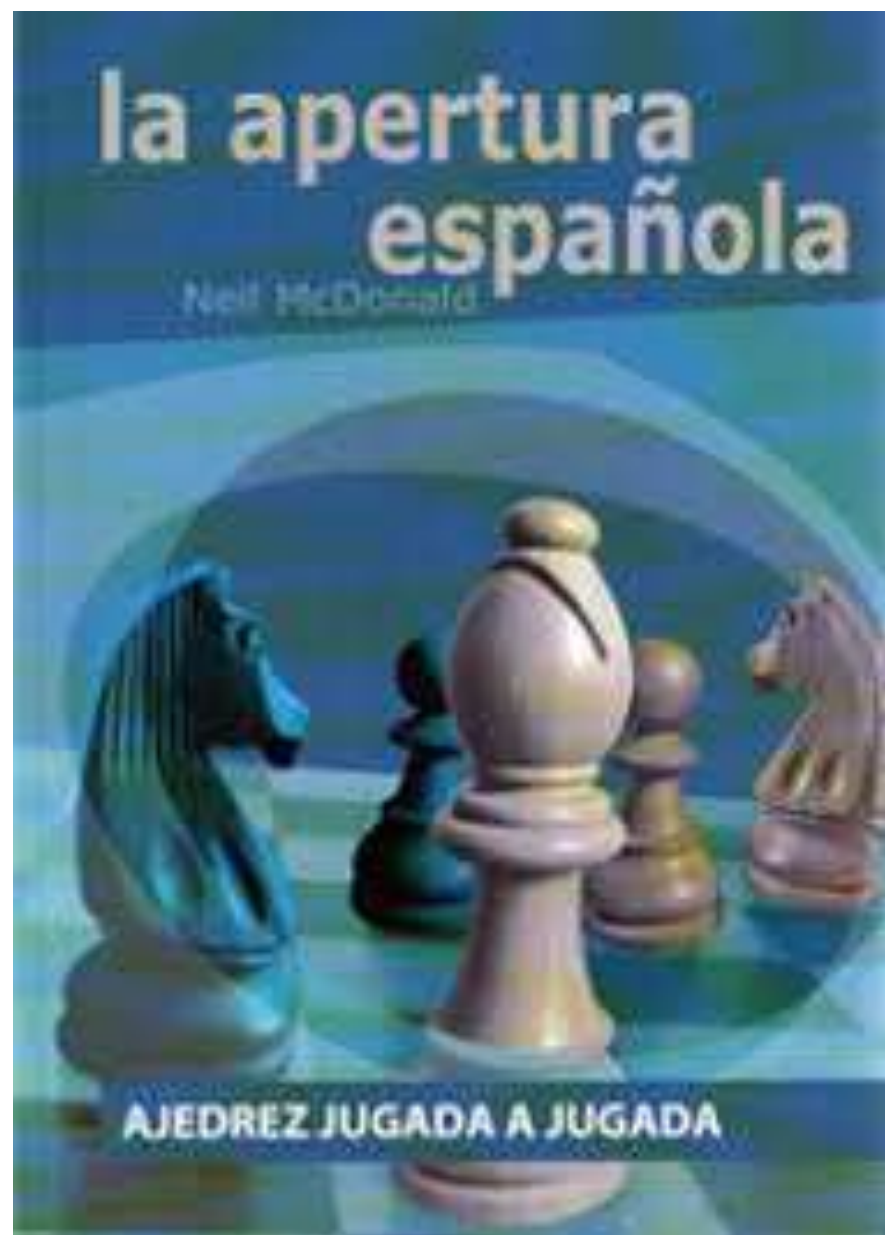
**No existe la bala de plata ....**



**Debemos de apostar a una  
estrategia de ciber seguridad.**









Fecha de publicación: 2017-06-28

# Guatemala: Hackers atacan sitio web de la SAT; afecta pagos tributarios

Las fallas que tiene el portal web sat.gob.gt se debe a que hackers han atacado el sitio con la intención de inhabilitarlo, denunció el superintendente de esa institución, Juan Francisco Solórzano Foppa.



Por Prensa Libre

"Como institución estamos trabajando para seguir ofreciendo los servicios a la población de forma confiable y sin inconvenientes", informó la Superintendencia de Administración Tributaria (SAT), en un comunicado.

La institución informa que está coordinando de forma permanente con las empresas proveedoras de esta conectividad para garantizar la disponibilidad de los servicios. Además, se han activado todos los protocolos de seguridad informática para protegerlos de los ataques.

## El superintendente confirmó que el sistema informático ha sido blanco de ataques cibernéticos.

La SAT informó que denunciará el caso del ataque informático ante el Ministerio Público. La denuncia será por los delitos de Atentado contra la seguridad de servicios de utilidad pública e Interrupción o entorpecimiento de comunicación (artículos 294 y 295 del Código Penal).

Mié 8 May 2018 Actualizado 18:15h

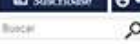


17° 22° 14°

PRENSA LIBRE

Un periodismo independiente, honesto y digno

Suscribirse



Economía

## El 80% de ciberataques se genera en las empresas

La necesidad de cuidar la seguridad informática no debe pasar inadvertida, se deben crear leyes, y hábitos de la vida real.

Por Rosa María Bolaños / Guatemala

7 de Septiembre de 2017 a las 14:53h



Aplicar medidas y adoptar patrones de cuidado se han convertido en herramientas obligatorias para evitar ser atacados por posibles virus informáticos.

Andrés Velázquez presidente y fundador de Mattica, que se presenta como el primer laboratorio forense de investigaciones digitales de Latinoamérica, visitó Guatemala para hablar de la vulnerabilidad en los sistemas informáticos, y la forma en cómo las empresas guatemaltecas pueden prepararse ante posibles ataques de este tipo.



LEA MÁS EN

Impulse la cultura para lograr seguridad informática



### ¿De dónde provienen los ataques?

Hemos detectado que el 80% de los casos que atendemos provienen del propio personal de las empresas. De ese porcentaje, el 36% tiene que ver con robos de secretos industriales, incluso hemos comprobado que la información se lleva de la organización en una USB.

### Esta última parte ¿tiene que ver con ciberseguridad?

Sí, un delito informático es toda aquella conducta que se puede tipificar en donde el medio de comisión o el fin es un elemento tecnológico. Un fraude en internet, por ejemplo, es un cibercrimen, porque se usa en los medios digitales.

## Economía

# Hackers atacan sitio web de la SAT; afecta pagos tributarios

Las fallas que tiene el portal web sat.gob.gt se debe a que hackers han atacado el sitio con la intención de inhabilitarlo, denunció el superintendente de esa institución, Juan Francisco Solórzano Foppa.

Por Natiana Gándara

27 de Junio de 2017 a las 17:48h





Secure | https://www.shodan.io

Shodan Developers Book View All... Show API Key Help Center

SHODAN country:ni port:7071 hostname:gob.ni

Explore Downloads Reports Developer Pricing Enterprise Access Contact Us My Account

# The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



## Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



## See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



## Monitor Network Security

Keep track of all the computers on your network that are



## Get a Competitive Advantage

Who is using your product? Where are they located? Use



# Find DNS Host Records

Find all Forward DNS ( [A](#) ) records for a domain. Enter a domain name and search for all subdomains associated with the domain. This is a reconnaissance tool when assessing an organisations security.

**FIND (A) RECORDS**



---- Protocolos inseguros publicados ----

country:ni	port:25	hostname:gob.ni	
country:ni	port:110	hostname:gob.ni	-- pop3
country:ni	port:143	hostname:gob.ni	-- imap4
country:ni	port:389	hostname:gob.ni	-- ldap

---- Protocolos seguros publicados ----

country:ni	port:465	hostname:gob.ni	-- smtps
country:ni	port:993	hostname:gob.ni	-- pop3s
country:ni	port:995	hostname:gob.ni	-- imap4s
country:ni	port:389	hostname:gob.ni	-- ldaps

## Zimbra

-----  
[https://wiki.zimbra.com/wiki/Firewall\\_Configuration](https://wiki.zimbra.com/wiki/Firewall_Configuration)

[https://wiki.zimbra.com/index.php?title=Best\\_Practices\\_on\\_Email\\_Protection:\\_SPF,\\_DKIM\\_and\\_DMARC](https://wiki.zimbra.com/index.php?title=Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC)

----- Servicios Peligrosos Publicados ----

country:ni port:7071 hostname:gob.ni

country:ni port:3389 hostname:gob.ni

country:ni port:21 hostname:gob.ni

---- Descubriendo DNS Server publicados ----

country:ni port:53 hostname:gob.ni

---- Descubriendo Sitios Web publicados ----

country:ni port:80 hostname:gob.ni

country:ni port:443 hostname:gob.ni

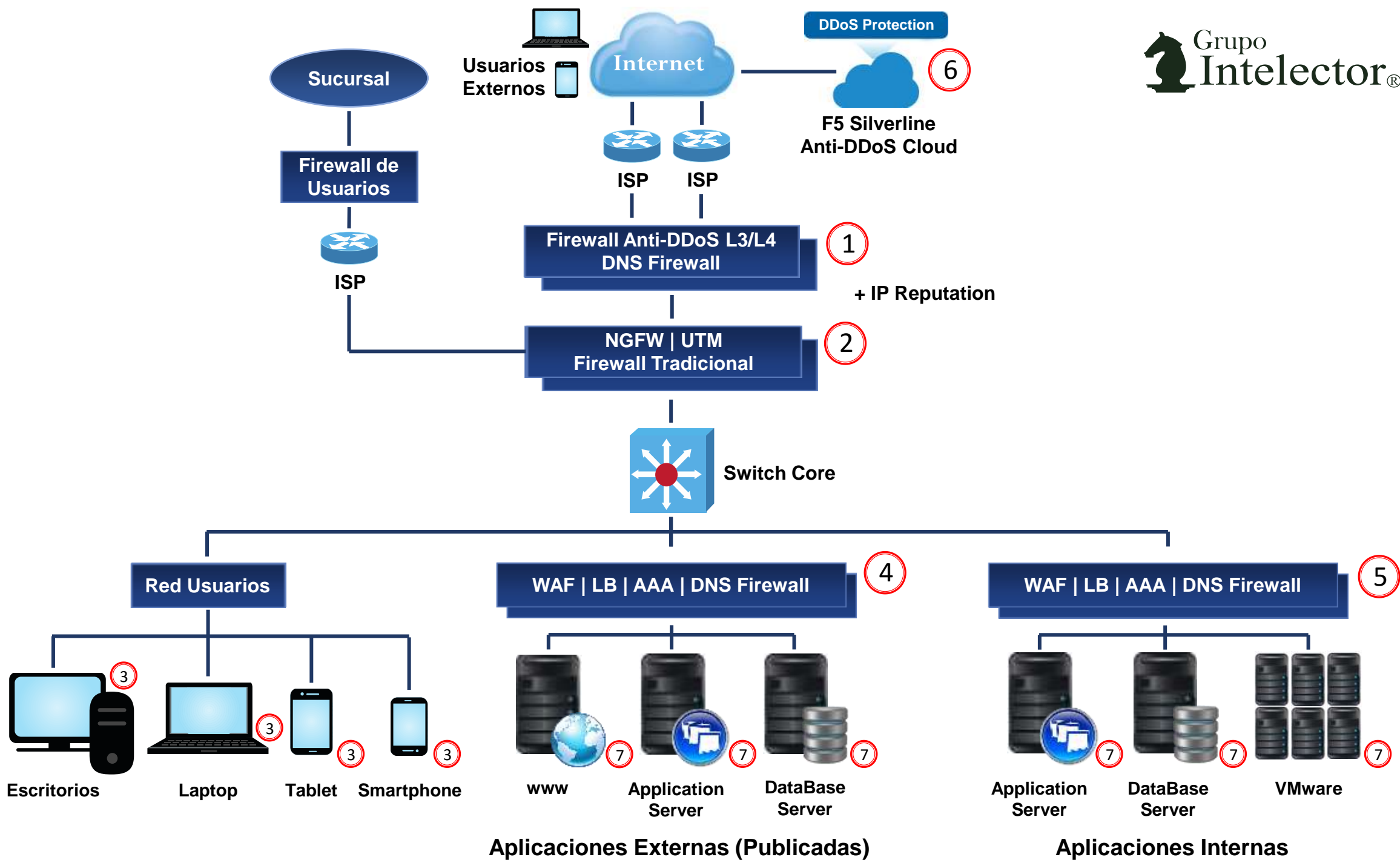
---- Descubriendo Webmail publicados -----

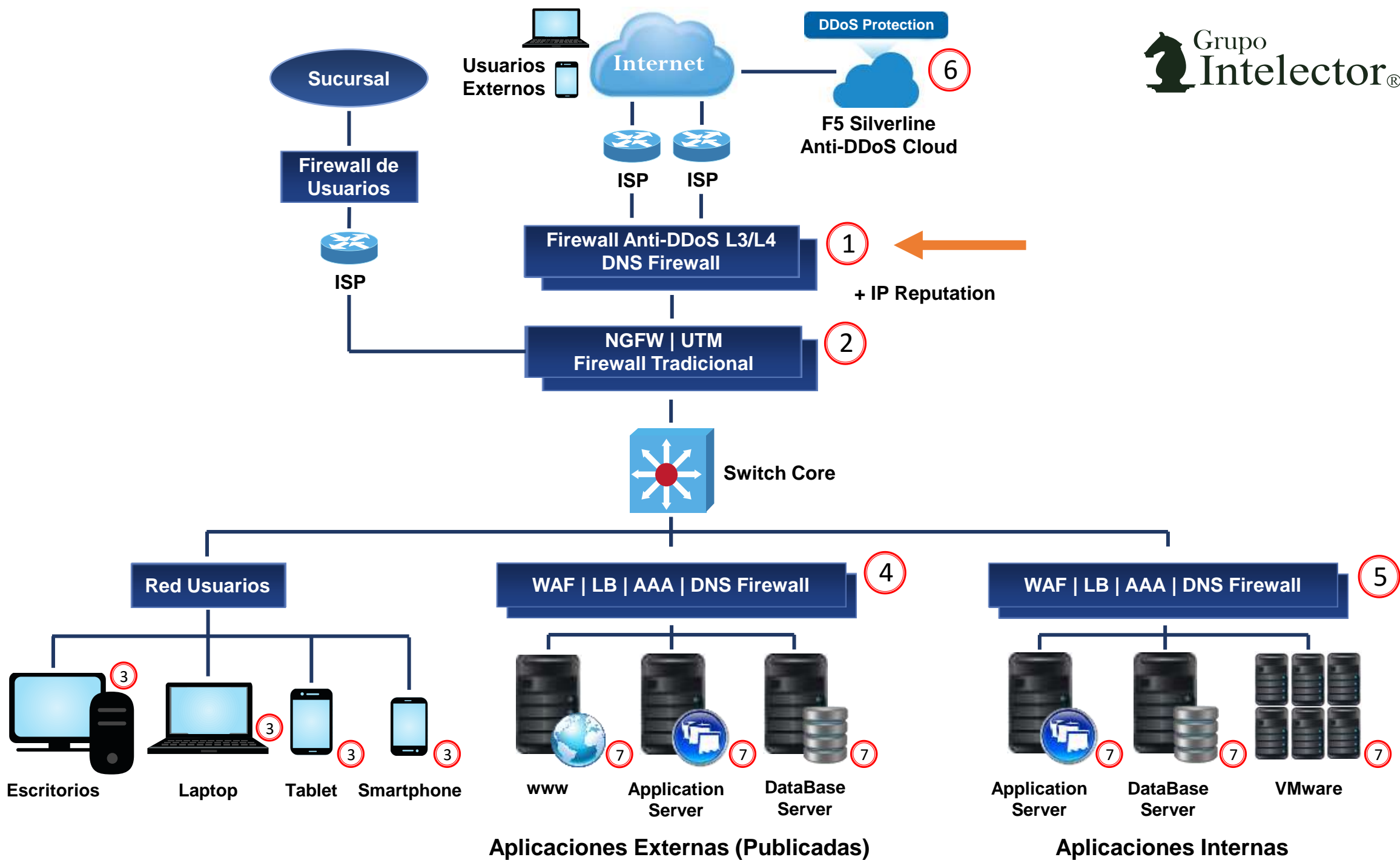
country:ni port:443 hostname:mail hostname:gob.ni

country:ni port:443 hostname:webmail hostname:gob.ni

country:ni port:443 hostname:corre hostname:gob.ni









# Ataques DDoS



<https://www.youtube.com/watch?v=OpFrCOfRo80>

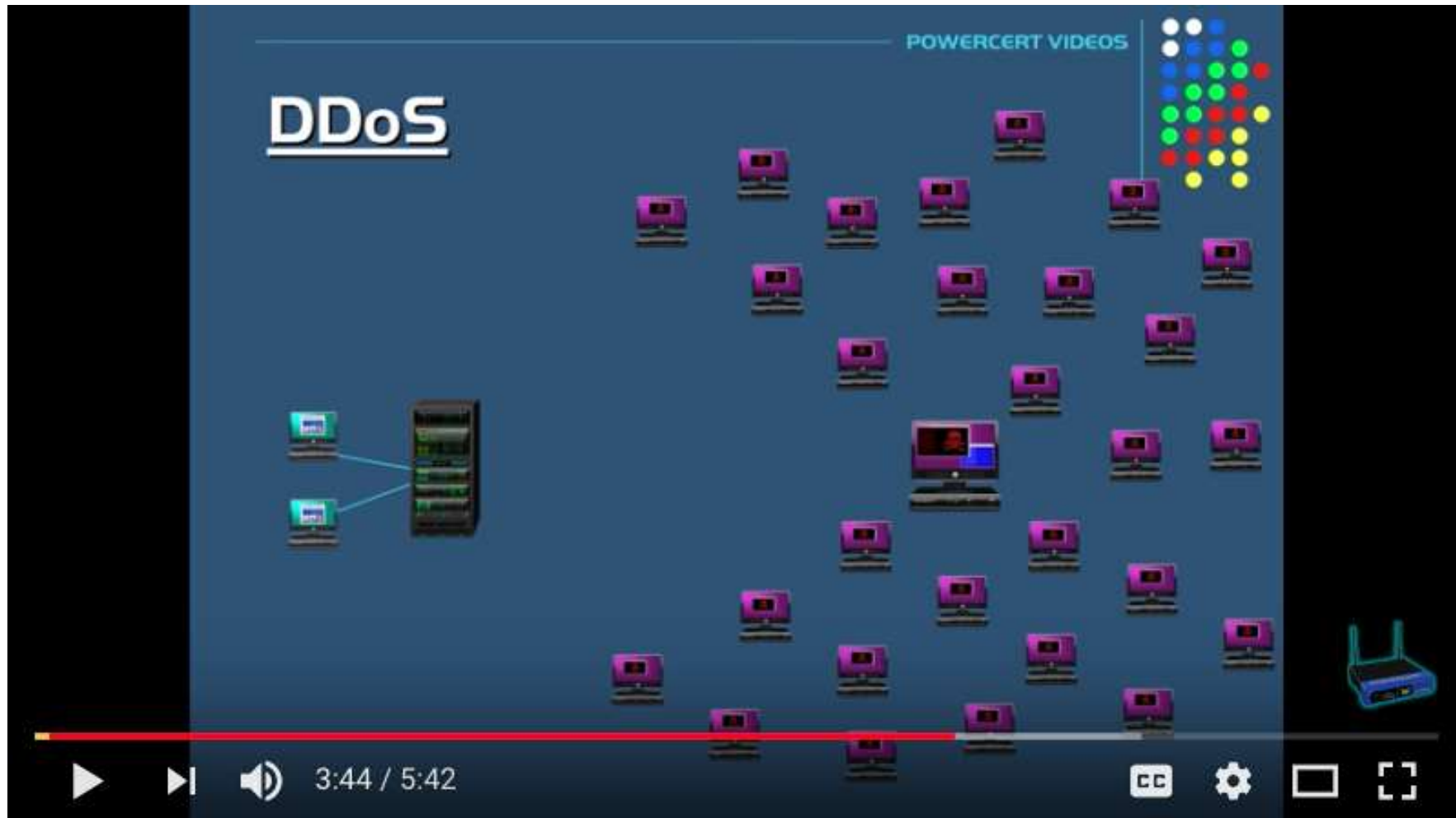
# Ataques DDoS



<https://www.youtube.com/watch?v=gqxKm8Fu4N8>



# Ataques DDoS



<https://www.youtube.com/watch?v=ilhGh9CEIwM>

## — Anatomy of a Successful DDoS Attack

### **Today's sophisticated DDoS Attackers will:**

1. Footprint (profile) the Web Presence
2. Scan the infrastructure and Web resources
3. Initiate network-level volumetric attack
4. Test if Web Presence is impacted
5. Maintain Flood – spoof all source IPs
6. Initiate low-and-slow application attacks
7. Initiate specially-crafted packet attacks
8. Initiate DNS reflective/amplified attacks
9. Attempt to exploit (compromise) downstream servers
10. Simultaneously launch as many types of attacks as possible
11. Not relent or subside – they stand very firm in their resolve



**A combined attack simply increases the chance of success!**

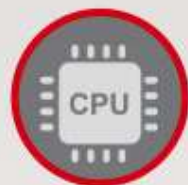


# DDoS Attack Targets



## Volumetric Attacks

Volumetric Attacks on Bandwidth



## Attacks on CPU

Attacks on CPU.  
IPS Signature Scanning.



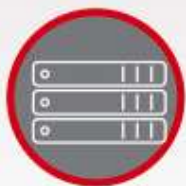
## Attacks on crypto

Attacks on crypto capacity.  
SSL floods.



## Attacks on RAM

Attacks on RAM. Firewall state tables.



## Attacks on Server

Attacks on Server stack. Low and Slow.



## Targeted Attacks

Targeted Attacks.  
Bugs and flaws in stack.

# Ataques DDoS



## 1. Volumetric Attacks (connectionless)

Also known as “floods,” the goal of this type of attack is to cause congestion and send so much traffic that it overwhelms the bandwidth of the site. Attacks are typically executed using botnets, an army of computers infected with malicious software and controlled as a group by the hacker.

## 2. TCP State-Exhaustion Attacks

This type of attack focuses on actual web servers, firewalls and load balancers to disrupt connections, resulting in exhausting their finite number of concurrent connections the device can support.

## 3. Application Layer Attacks (connection-based)

This type of attack, also known as Layer 7 attacks, specifically targets weaknesses in an application or server with the goal of establishing a connection and exhausting it by monopolizing processes and transactions. These sophisticated threats are harder to detect because not many machines are required to attack, generating a low traffic rate that appears to be legitimate.



## 1. Application Level Attacks

DDoS attacks can target a specific application or a badly coded website to exploit its weakness and take down the entire server as a result. WordPress and Joomla are two examples of applications that can be targeted to exhaust a server's resources – RAM, CPU, etc. Databases can also be targeted with SQL injections designed to exploit these loopholes.

The exhausted server is then unavailable to process legitimate requests due to exhausted resources. Websites and applications with security loopholes are also susceptible to hackers looking to steal information.

## 2. Zero Day (0day) DDoS

This is a standard term (like John Doe) used to describe an attack that is exploiting new vulnerabilities. These ZERO Day DDoS vulnerabilities do not have patches or effective defensive mechanisms.

## 3. Ping Flood

An evolved version of ICMP flood, this DDoS attack is also application specific. When a server receives a lot of spoofed Ping packets from a very large set of source IP it is being targeted by a Ping Flood attack. Such an attack's goal is to flood the target with ping packets until it goes offline.

It is designed to consume all available bandwidth and resources in the network until it is completely drained out and shuts down. This type of DDoS attack is also not easy to detect as it can easily resemble legitimate traffic.

## 4. IP Null Attack

Packets contain IPv4 headers which carry information about which Transport Protocol is being used. When attackers set the value of this field to zero, these packets can bypass security measures designed to scan TCP, IP, and ICMP. When the target server tries to process these packets, it will eventually exhaust its resources and reboot.

## 5. CharGEN Flood

It is a very old protocol which can be exploited to execute amplified attacks. A CharGEN amplification attack is carried out by sending small packets carrying a spoofed IP of the target to internet enabled devices running CharGEN. These spoofed requests to such devices are then used to send UDP floods as responses from these devices to the target.

Most internet-enabled printers, copiers etc., have this protocol enabled by default and can be used to execute a CharGEN attack. This can be used to flood a target with UDP packets on port 19. When the target tries to make sense of these requests, it will fail to do so. The server will eventually exhaust its resources and go offline or reboot.

## 6. SNMP Flood

Like a CharGEN attack, SNMP can also be used for amplification attacks. SNMP is mainly used on network devices. SNMP amplification attack is carried out by sending small packets carrying a spoofed IP of the target to the internet enabled devices running SNMP.

These spoofed requests to such devices are then used to send UDP floods as responses from these devices to the target. However, amplification effect in SNMP can be greater when compared with CHARGEN and DNS attacks. When the target tries to make sense of this flood of requests, it will end up exhausting its resources and go offline or reboot.

## 7. NTP Flood

The NTP protocol is another publicly accessible network protocol. The NTP amplification attack is also carried out by sending small packets carrying a spoofed IP of the target to internet enabled devices running NTP.

These spoofed requests to such devices are then used to send UDP floods as responses from these devices to the target. When the target tries to make sense of this flood of requests, it will end up exhausting its resources and go offline or reboot.



## 8. SSDP Flood

SSDP enabled network devices that are also accessible to UPnP from the internet are an easy source for generating SSDP amplification floods. The SSDP amplification attack is also carried out by sending small packets carrying a spoofed IP of the target to devices.

These spoofed requests to such devices are used to send UDP floods as responses from these devices to the target. When the target tries to make sense of this flood of requests, it will end up exhausting its resources and go offline or reboot.

## 9. Other Amplified DDoS Attacks

All amplified attacks use the same strategy described above for CHARGEN, NTP, etc. Other UDP protocols that have been identified as possible tools for carrying out amplification flood attacks U.S. CERT are:

- SNMPv2
- NetBIOS
- QOTD
- BitTorrent
- Kad
- Quake Network Protocol
- Steam Protocol

## 10. Fragmented HTTP Flood

In this example of a sophisticated attack on a known loophole, BOTs with a valid IP are used to establish a valid HTTP connection with a web server. Then, HTTP packets are split by the bot into tiny fragments and sent to the target as slowly as it allows before it times out. This method allows the attackers to keep a connection active for a long time without alerting any defense mechanisms.

An attacker can use one BOT to initiate several undetected, extended and resource consuming sessions. Popular web servers like Apache do not have effective timeout mechanisms. This is a DDoS security loophole that can be exploited with a few BOTs to stop web services.

## 11. HTTP Flood

The real IP of the BOTs is used to avoid suspicion. The number of BOTs used to execute the attack is same as the source IP range for this attack. Since the IP addresses of the BOTs are not spoofed, there is no reason for defense mechanisms to flag these valid HTTP requests.

One BOT can be used to send a large number of GET, POST or other HTTP requests to execute an attack. Several bots can be combined in an HTTP DDoS attack to completely cripple the target server.

## 12. Single Session HTTP Flood

An attacker can exploit a loophole in HTTP 1.1 to send several requests from a single HTTP session. This allows attackers to send a large number of requests from a handful of sessions. In other words, attackers can bypass the limitations imposed by DDoS defense mechanisms on the number of sessions allowed.

Single Session HTTP Flood also targets a server's resources to trigger a complete system shutdown or poor performance.

## 13. Single Request HTTP Flood

When defense mechanisms evolved to block many incoming packets, attacks like Single Packet HTTP Flood were designed with workarounds to dodge these defenses. This evolution of an HTTP flood exploits another loophole in the HTTP technology. Several HTTP requests can be made by a single HTTP session by masking these requests within one HTTP packet.

This technique allows an attack to stay invisible while exhausting a server's resources by keeping packet rates within the allowed limits.



## **14. Recursive HTTP GET Flood**

For an attack to be highly successful, it must remain undetected for as long as possible. The best method to go undetected is to appear as a legitimate request by staying within all the limitations while another attack is being executed. Recursive GET achieves this on its own by collecting a list of pages or images and appearing to be going through these pages or images.

This attack can be combined with an HTTP flood attack for maximum impact.

## **15. Random Recursive GET Flood**

This attack is a purpose built variation of Recursive GET attack. It is designed for forums, blogs and other websites that have pages in a sequence. Like Recursive GET it also appears to be going through pages. Since page names are in a sequence, to keep up appearance as a legitimate user, it uses random numbers from a valid page range to send a new GET request each time.

Random Recursive GET also aims to deflate its target's performance with a large number of GET requests and deny access to real users.

## 16. Multi-Vector Attacks

We talked about attackers combining Recursive GET attacks with HTTP flood attacks to amplify the effects of an attack. That's just one example of an attacker using two types of DDoS attacks at the same time to target a server. Attacks can also combine several methods to keep the engineers dealing with the DDoS attack confused.

These attacks are the toughest to deal with and are capable of taking down some of the best-protected servers and networks.

## 17. SYN Flood

This attack exploits the design of the three-way TCP communication process between a client, host, and a server. In this process, a client initiates a new session by generating a SYN packet. The host assigns and checks these sessions until they are closed by the client. To carry out a SYN Flood attack, an attacker sends a lot of SYN packets to the target server from spoofed IP addresses.

This attack goes on until it exhausts a server's connection table memory –stores and processes these incoming SYN packets. The result is a server unavailable to process legitimate requests due to exhausted resources until the attack lasts.

## **18. SYN-ACK Flood**

The second step of the three-way TCP communication process is exploited by this DDoS attack. In this step, a SYN-ACK packet is generated by the listening host to acknowledge an incoming SYN packet. A large amount of spoofed SYN-ACK packets is sent to a target server in a SYN-ACK Flood attack. The attack tries to exhaust a server's resources – its RAM, CPU, etc. as the server tries to process this flood of requests.

The result is a server unavailable to process legitimate requests due to exhausted resources until the attack lasts.

## **19. ACK & PUSH ACK Flood**

During an active TCP-SYN session, ACK or PUSH ACK packets carry information to and from the host and client machines till the session lasts. During an ACK & PUSH ACK flood attack, a large amount of spoofed ACK packets is sent to the target server to deflate it.

Since these packets are not linked with any session on the server's connection list, the server spends more resources on processing these requests. The result is a server unavailable to process legitimate requests due to exhausted resources until the attack lasts.



## 20. ACK Fragmentation Flood

Fragmented ACK packets are used in this bandwidth consuming version of the ACK & PUSH ACK Flood attack. To execute this attack, fragmented packets of 1500 bytes are sent to the target server. It is easier for these packets to reach their target undetected as they are not normally reassembled by routers at the IP level.

This allows an attacker to send few packets with irrelevant data through routing devices to consume large amounts of bandwidth. This attack affects all servers within the target network by trying to consume all available bandwidth in the network.

## 21. RST/FIN Flood

After a successful three or four-way TCP-SYN session, RST or FIN packets are exchanged by servers to close the TCP-SYN session between a host and a client machine. In an RST or FIN Flood attack, a target server receives a large number of spoofed RST or FIN packets that do not belong to any session on the target server.

The attack tries to exhaust a server's resources – its RAM, CPU, etc. as the server tries to process these invalid requests. The result is a server unavailable to process legitimate requests due to exhausted resources.

## 22. Synonymous IP Attack

To take a server down, a large number of TCP-SYN packets carrying the target server's Source IP and Destination IP are sent to the target server. Even though the packets are carrying the target server's source and destination IP information, this data is not important.

The goal of the Synonymous IP attack is to exhaust a server's resources – RAM, CPU, etc. as it tries to compute this anomaly. The exhausted server is then unavailable to process legitimate requests due to exhausted resources.

## 23. Spoofed Session Flood

Some of the above DDoS attacks are unable to fool most modern defense mechanisms but DDoS attacks are also evolving to bypass these defenses. Fake Session attacks try to bypass security under the disguise of a valid TCP session by carrying a SYN, multiple ACK and one or more RST or FIN packets.

This attack can bypass defense mechanisms that are only monitoring incoming traffic on the network. These DDoS attacks can also exhaust the target's resources and result in a complete system shutdown or unacceptable system performance.

## 24. Multiple SYN-ACK Spoofed Session Flood

This version of a fake session attack contains multiple SYN and multiple ACK packets along with one or more RST or FIN packets. A Multiple SYN-ACK Fake Session is another example of an evolved DDoS attack. They are changed up to bypass defense mechanisms which rely on very specific rules to prevent such attacks.

Like the Fake Session attack, this attack can also exhaust a target's resources and result in a complete system shutdown or unacceptable system performance.

## 25. Multiple ACK Spoofed Session Flood

SYN is completely skipped in this version of Fake Session. Multiple ACK packets are used to begin and carry an attack. These ACK packets are followed by one or more RST or FIN packets to complete the disguise of a TCP session.

These attacks tend to be more successful at staying under the radar as they generate low TCP-SYN traffic compared to the original SYN-Flood attacks. Like its source, the Multiple ACK Fake Session attack can also exhaust a target's resources and result in a complete system shutdown or unacceptable system performance.



## 26. Session Attack

To bypass defenses, instead of using spoofed IPs, this attack uses the real IP address of the BOTs being used to carry out an attack. The number of BOTs used to execute the attack is same as the source IP range for this attack. This attack is executed by creating a TCP-SYN session between a BOT and the target server.

This session is then stretched out until it times out by delaying the ACK packets. Session attacks try to exhaust a server's resources through these empty sessions. That, in turn, results in a complete system shutdown or unacceptable system performance.

## 27. Misused Application Attack

The attackers first hack client machines that host high traffic apps like P2P services. The traffic from these client machines is then redirected to the target server. The target server exhausts its resources as it tries to accept and negotiate the excessive traffic. Defensive mechanisms aren't triggered in this case as the hacked client machines are actually trying to make a valid connection to the target server.

After successfully redirecting the traffic to the target, as the attack is going on, the attacker drops off the network and becomes untraceable. Misused Application Attack targets a server's resources and tries to take it down or destroy its performance.

## 28. UDP Flood

As the name suggests, in this type of DDoS attack a server is flooded with UDP packets. Unlike TCP, there isn't an end to end process of communication between client and host. This makes it harder for defensive mechanisms to identify a UDP Flood attack. A large number of spoofed UDP packets are sent to a target server from a massive set of source IP to take it down.

UDP flood attacks can target random servers or a specific server within a network by including the target server's port and IP address in the attacking packets. The goal of such an attack is to consume the bandwidth in a network until all available bandwidth has been exhausted.

## 29. UDP Fragmentation Flood

It is another one of those cleverly masked DDoS attacks that are not easily detected. The activity generated by this attack resembles valid traffic and all of it is kept within limits. This version of the UDP Flood attack sends larger yet fragmented packets to exhaust more bandwidth by sending fewer fragmented UDP packets.

When a target server tries to put these unrelated and forged fragmented UDP packets together, it will fail to do so. Eventually, all available resources are exhausted and the server may reboot.

## 30. DNS Flood

One of the most well-known DDoS attacks, this version of UDP flood attack is application specific – DNS servers in this case. It is also one of the toughest DDoS attacks to detect and prevent. To execute, an attacker sends a large amount of spoofed DNS request packets that look no different from real requests from a very large set of source IP.

This makes it impossible for the target server to differentiate between legitimate DNS requests and DNS requests that appear to be legitimate. In trying to serve all the requests, the server exhausts its resources. The attack consumes all available bandwidth in the network until it is completely drained out.

## 31. VoIP Flood

This version of application specific UDP flood targets VoIP servers. An attacker sends a large number of spoofed VoIP request packets from a very large set of source IP. When a VoIP server is flooded with spoofed requests, it exhausts all available resources while trying to serve the valid and invalid requests. This reboots the server or takes a toll on the server's performance and exhausts the available bandwidth. VoIP floods can contain fixed or random source IP. Fixed source IP address attack is not easy to detect as it masks itself and looks no different from legitimate traffic.



## 32. Media Data Flood

Like VoIP flood, a server can also be attacked with media data such as audio and video. A large number of spoofed media data packets are sent by an attacker from a very large set of source IP. When a server is flooded with spoofed media data requests, it exhausts all available resources and network bandwidth to process these requests.

This attack is similar to VoIP floods in every way other than using spoofed media data packets to attacks the server. It can also be hard to detect these attacks when they are using fixed source IP as this gives them a legitimate appearance. The attack is designed to consume all available server resources and bandwidth in the network until it is completely drained out.

## 33. Direct UDP Flood

The target server is attacked with a large number of Non-Spoofed UDP packets. To mask the attack, the attacker does not spoof the BOTs actual IP address. The number of BOTs used to execute the attack is same as the source IP range for this attack. The attack is designed to consume all available bandwidth and resources in the network until it is completely drained out and shuts down. This type of DDoS attack is also not easy to detect as it resembles legitimate traffic.

## 34. ICMP Flood

Like UDP, the ICMP stack also does not have an end to end process for data exchange. This makes it harder to detect an ICMP Flood attack. An attacker sends a large number of spoofed ICMP packets from a very large set of source IP. When a server is flooded with massive amounts of spoofed ICMP packets, its resources are exhausted in trying to process these requests. This overload reboots the server or has a massive impact on its performance.

ICMP flood attacks can target random servers or a specific server within a network by including the target server's port and IP address in the packets. The goal of such an attack is to consume bandwidth in the network until it has exhausted the available bandwidth.

## 35. ICMP Fragmentation Flood

This version of ICMP Flood attack sends larger packets to exhaust more bandwidth by sending fewer fragmented ICMP packets. When the target server tries to put these forged fragmented ICMP packets with no correlation together, it will fail to do so. The server eventually exhausts its resources and reboots.

# — Top Ten Tips

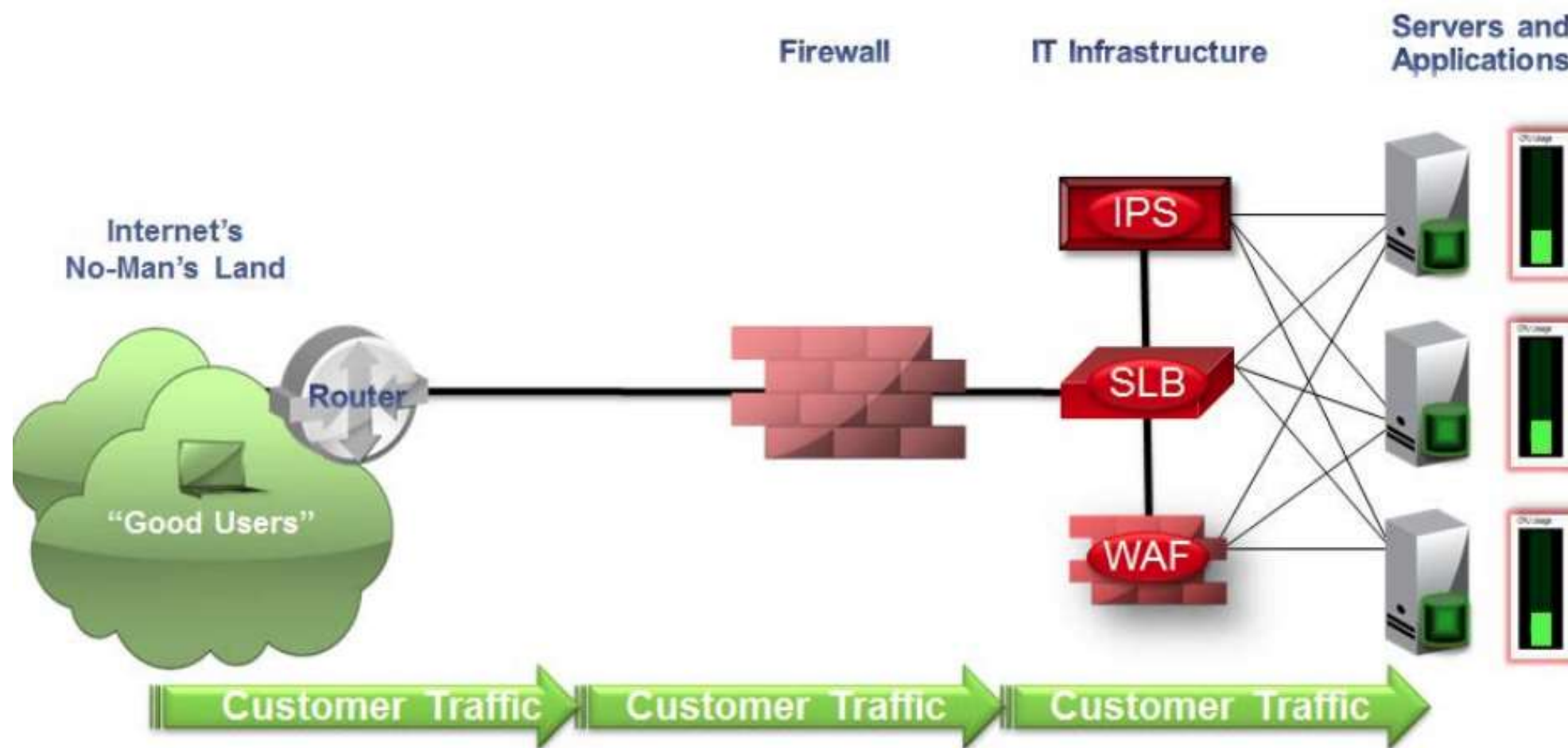
## **Your “First Line of Defense” Must Block:**

1. Known malicious IP addresses - constantly update reputation intelligence
2. Unwanted countries where you do not do business – current geolocation information
3. Botnet infected machines and DDoS'ers – allow yet monitor all real users
4. Application abusers and unwanted activities – enforce usage standards
5. All unnecessary ports and protocols – deep packet inspect all allowed services
6. Protocol anomalies and violations - enforce RFC & industry standards
7. Advanced evasion techniques - manage fragmentation/segmentation policies
8. Exploits designed for data exfiltration – stop focused attackers at the perimeter
9. Brute-force password attempts – log and alert any suspicious activity
10. Lack of information about the state of your perimeter – increase your visibility



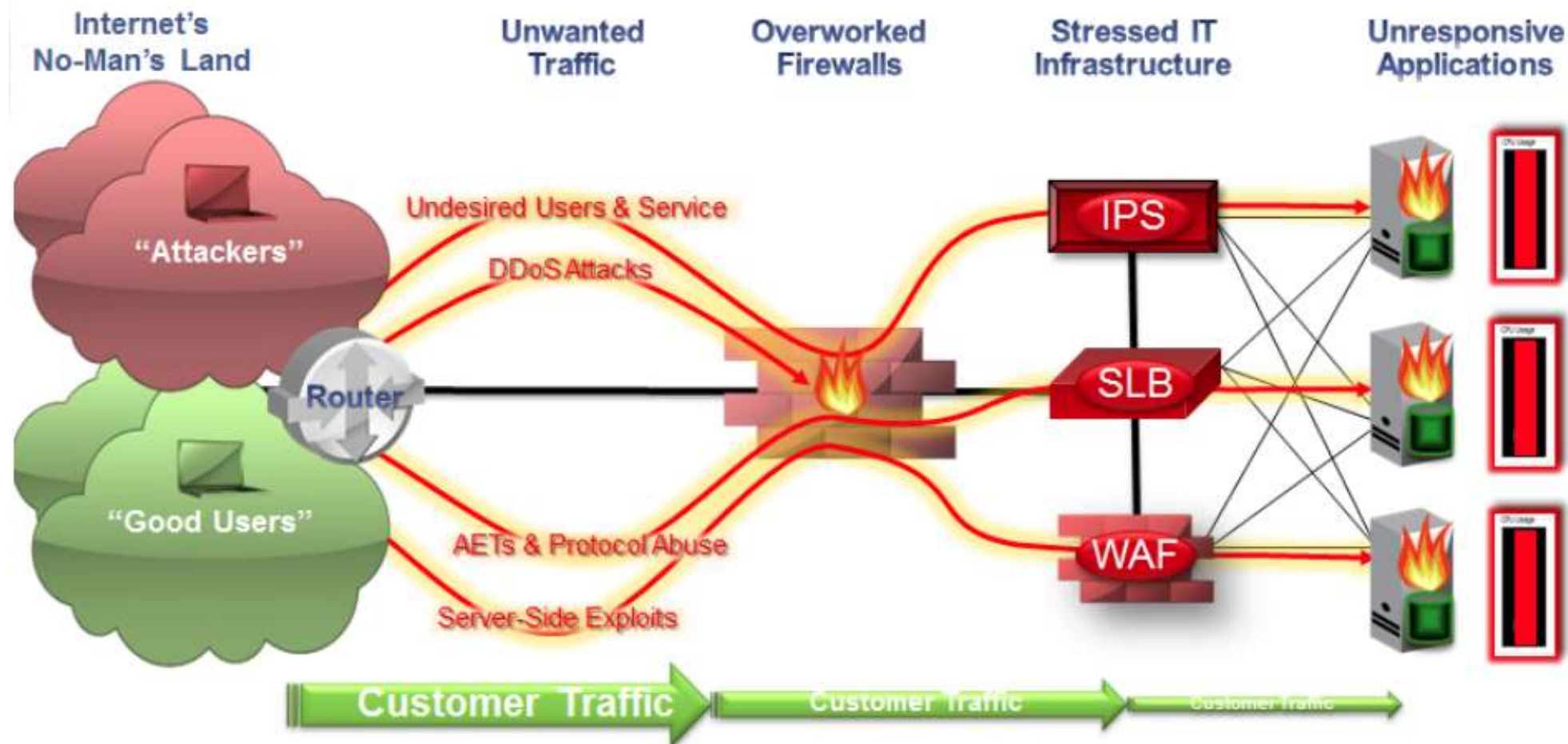


## — Typical Network Topology



**Assumption: Customer Traffic Flowing Through As Expected**

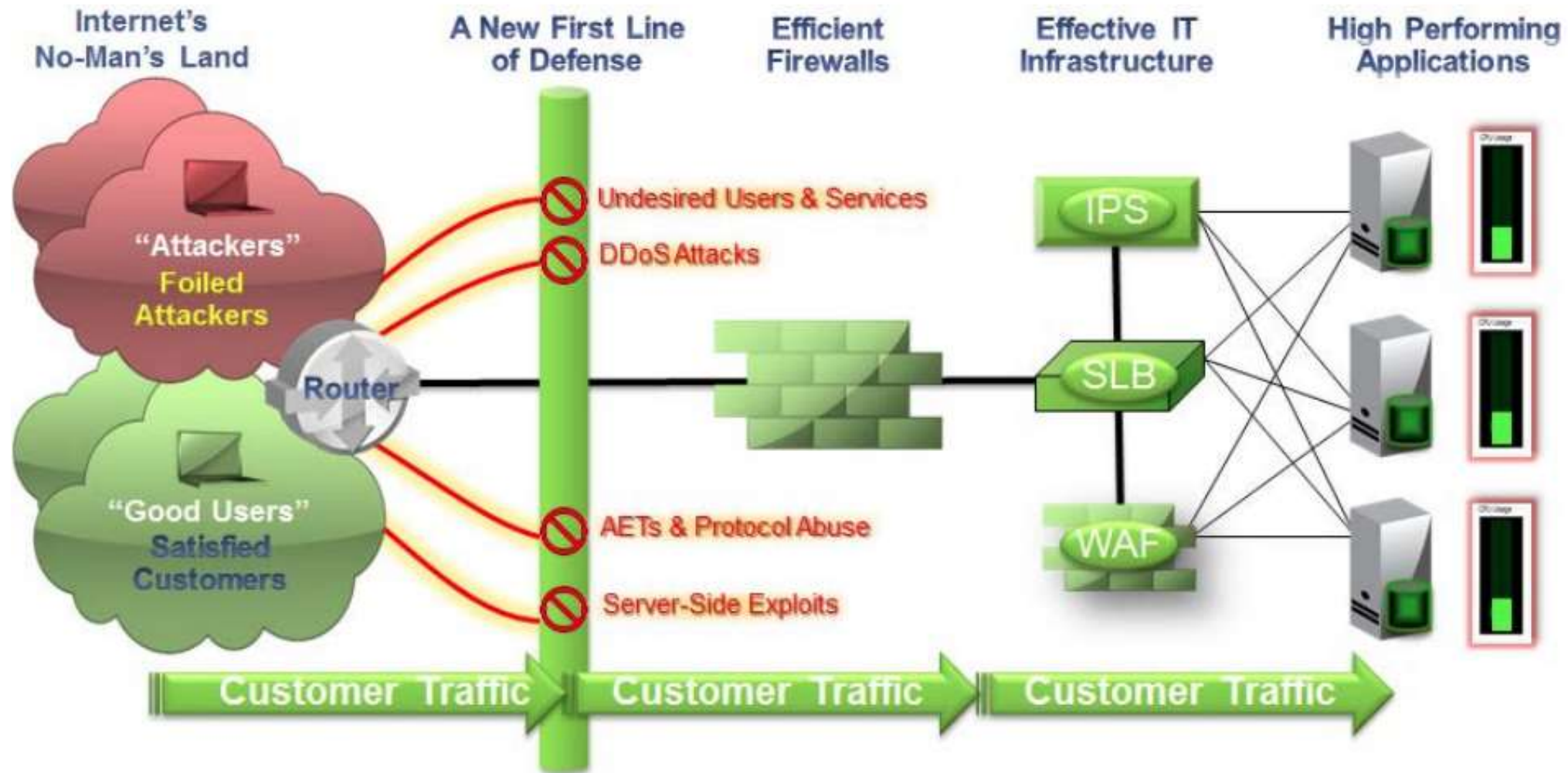
# — The Result of Unwanted Traffic



**Impacts: service degradation, site downtime, threat exposure, infrastructure overload, brand damage, lost business**



## — A New Way of Thinking!

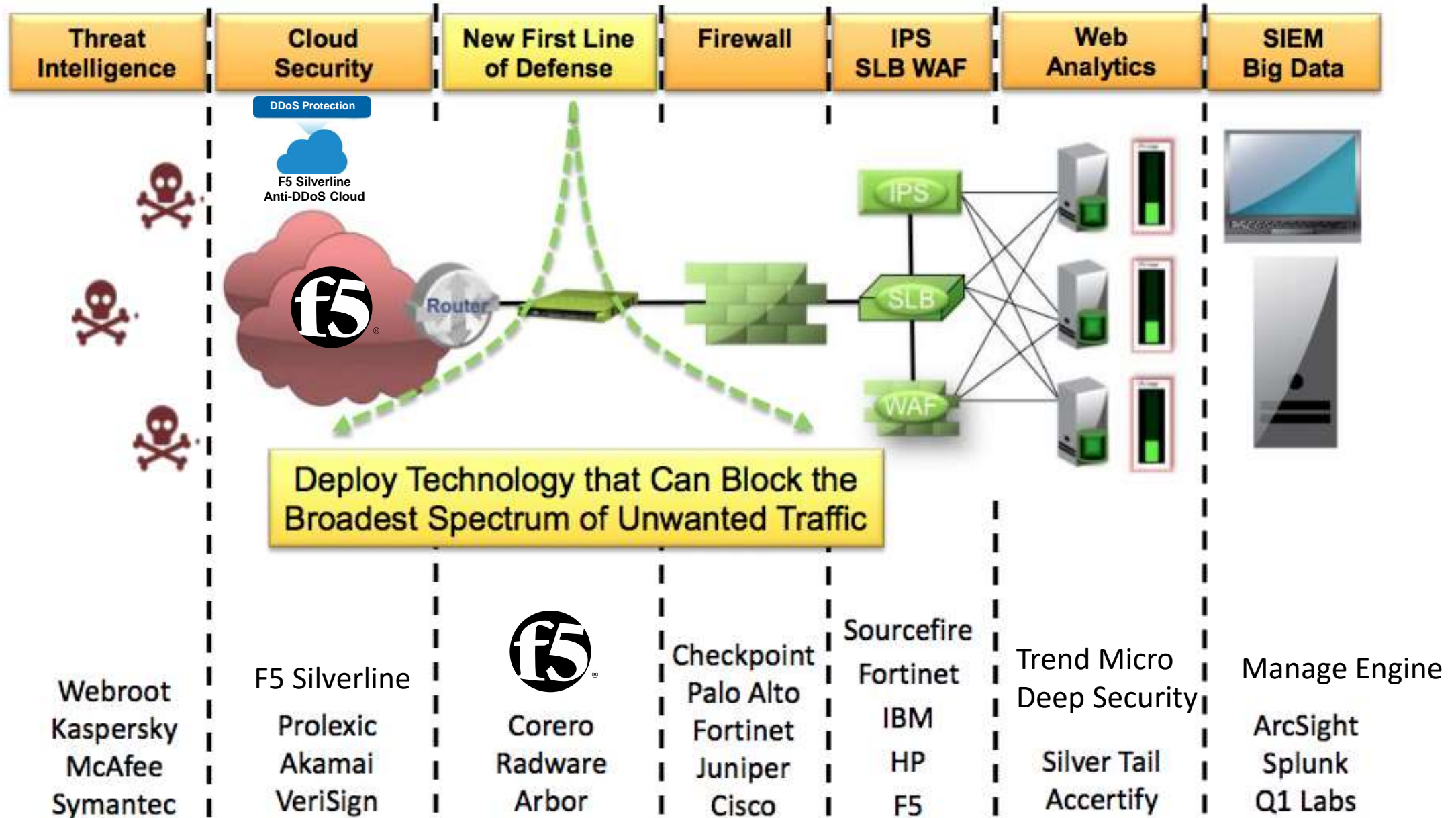


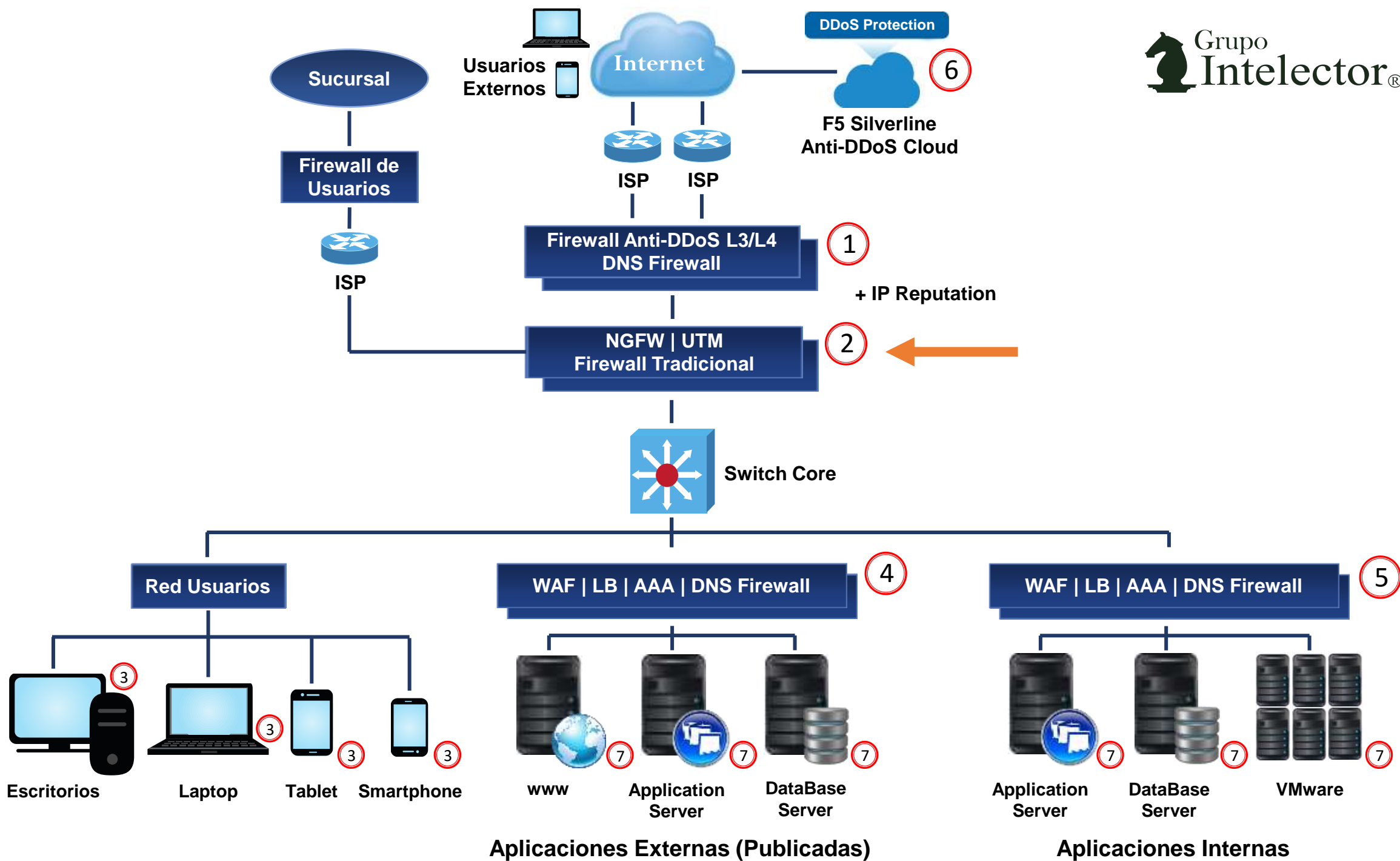
Protect your IT infrastructure by removing broad-based attacks FIRST!

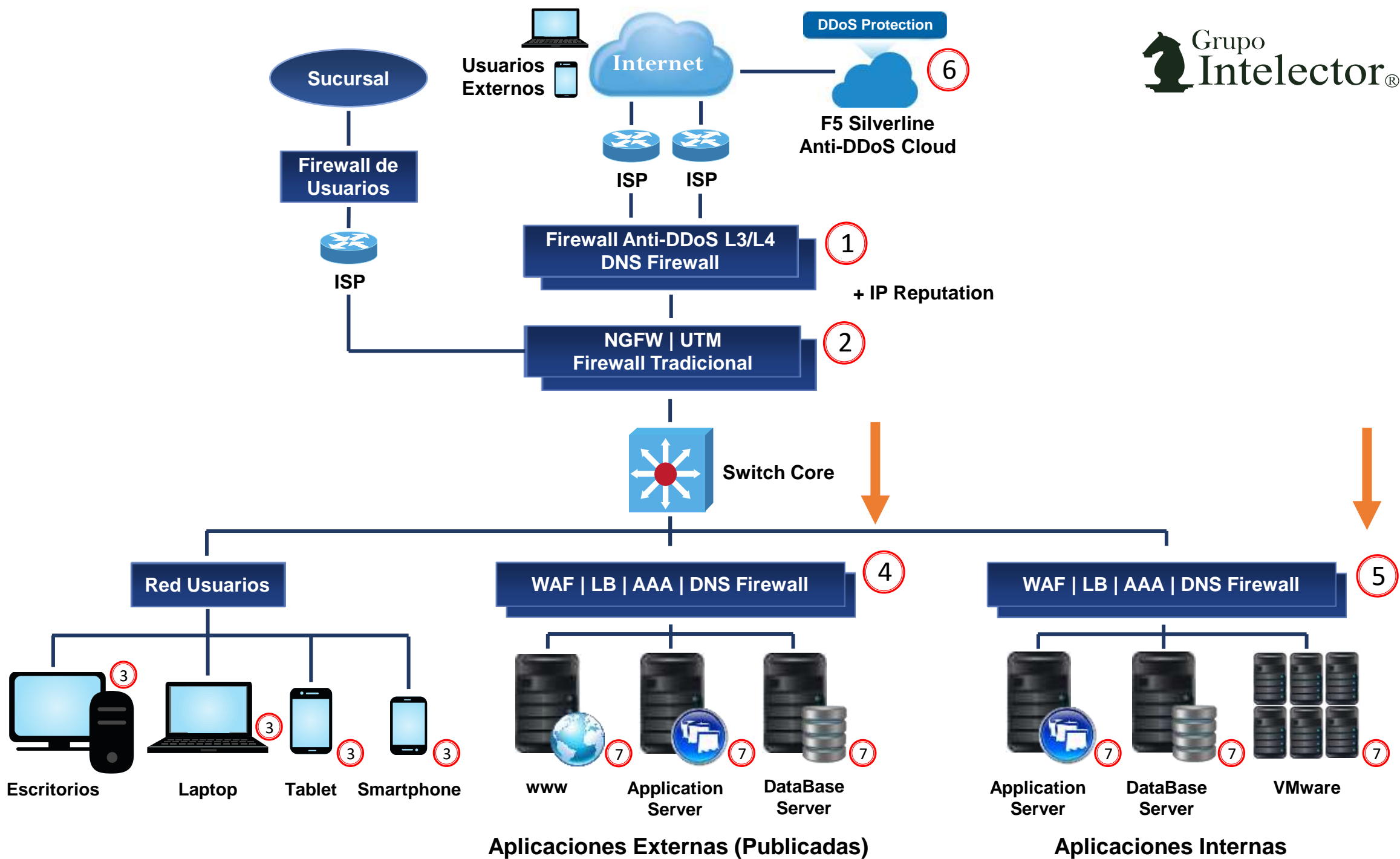


# Defense in Depth

r®









# Advanced vs Traditional Web Application Firewall

## TRADITIONAL WAF

- Signatures (OWASP Top 10)
- DAST integration
- Site learning
- File/URL/Parameter/Header/Cookie enforcement
- Protocol enforcement
- Login enforcement / Session tracking
- Data leak prevention
- Flow enforcement
- IP blacklisting

## ADVANCED WAF

- Bot detection
- Client fingerprinting
- Web scraping prevention
- Brute force mitigation
- L7 DDoS protection
- Heavy URL mitigation
- CAPTCHA challenges
- HTTP header sanitisation/insertion
- Anti-CSRF token insertion
- Perfect Forward Secrecy (PFS) ciphers

# Application Attacks are Inevitable

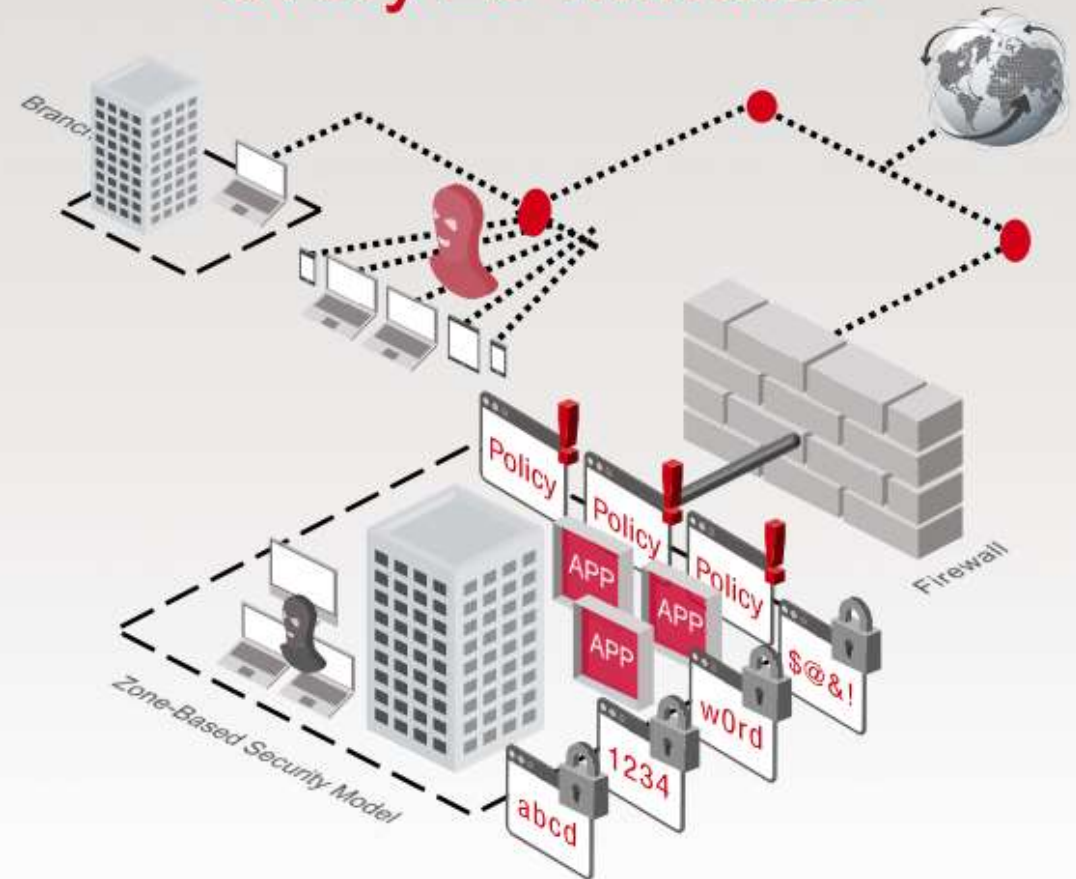
**75%** of Internet threats target web servers

**86%** of websites has at least 1 vulnerability and an average of 56 per website

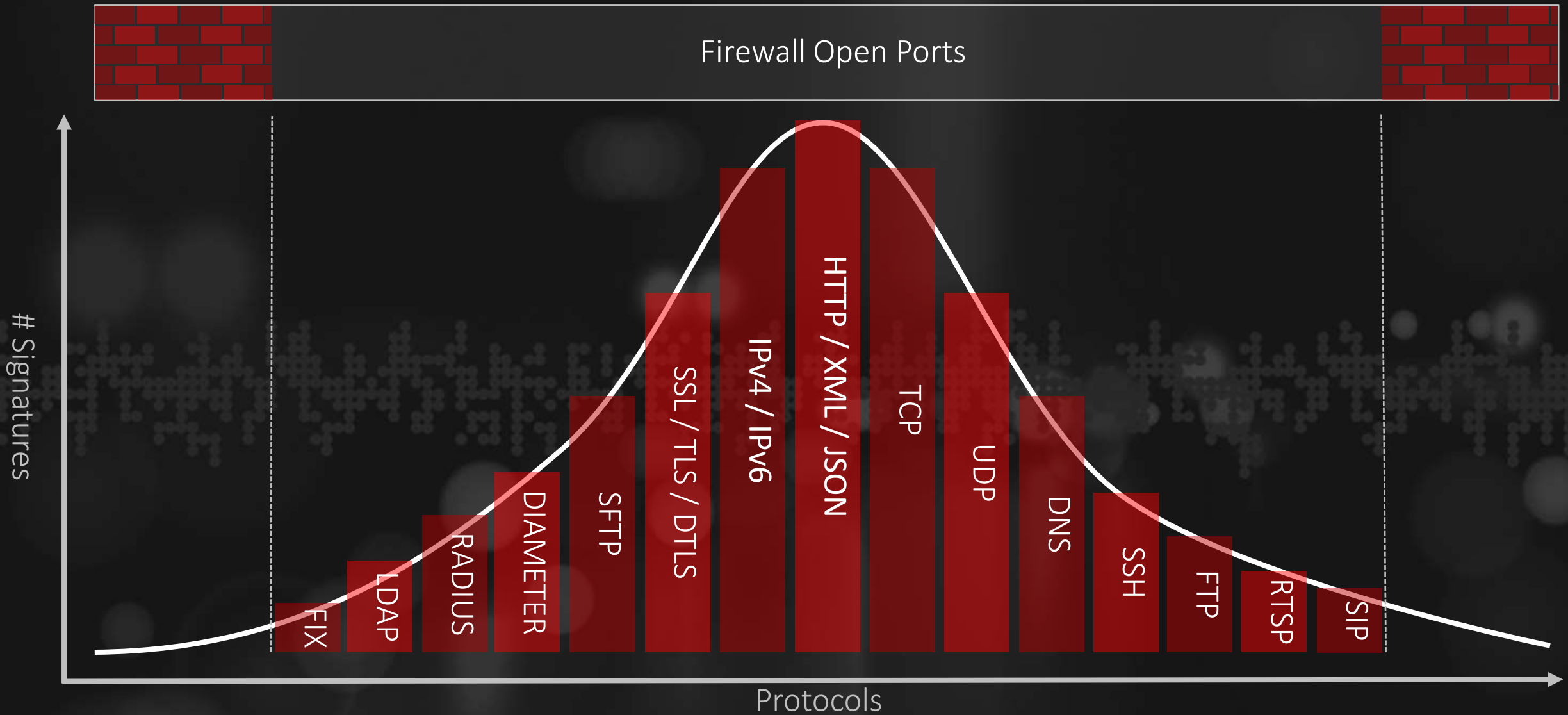
**95%** of breaches through 2018 will be **caused by misconfigured firewalls**, not vulnerabilities

**2.3M** bots actively attacking

Prepare for application attacks  
**every 23 minutes**



# F5 Full-Proxy Security vs IDS, IPS & NGFW





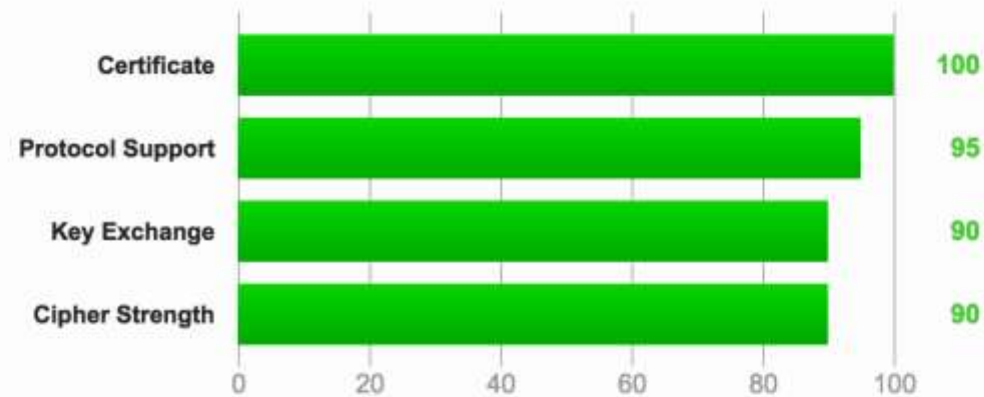
## SSL Report: [f5.com](https://f5.com) (104.219.105.148)

Assessed on: Thu, 29 Oct 2015 11:52:57 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)

### Summary

#### Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS\_FALLBACK\_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

# Application Security Not Addressed by Traditional Firewalls

**BIG-IP ASM delivers comprehensive protection against critical web attacks**

CSRF

OWASP top 10

Forceful browsing

Web scraping

SQL injections

Field manipulation

Cross-site scripting

Command injection

Bots

Cookie manipulation

Brute force attacks

Buffer overflows

Parameter tampering

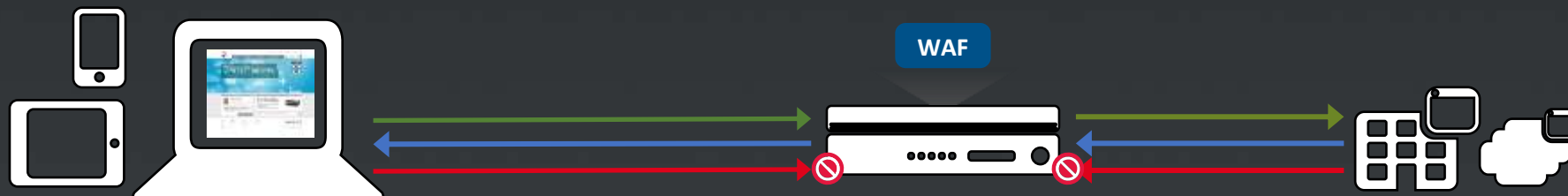
information leakage

Session high jacking

Zero-day attacks

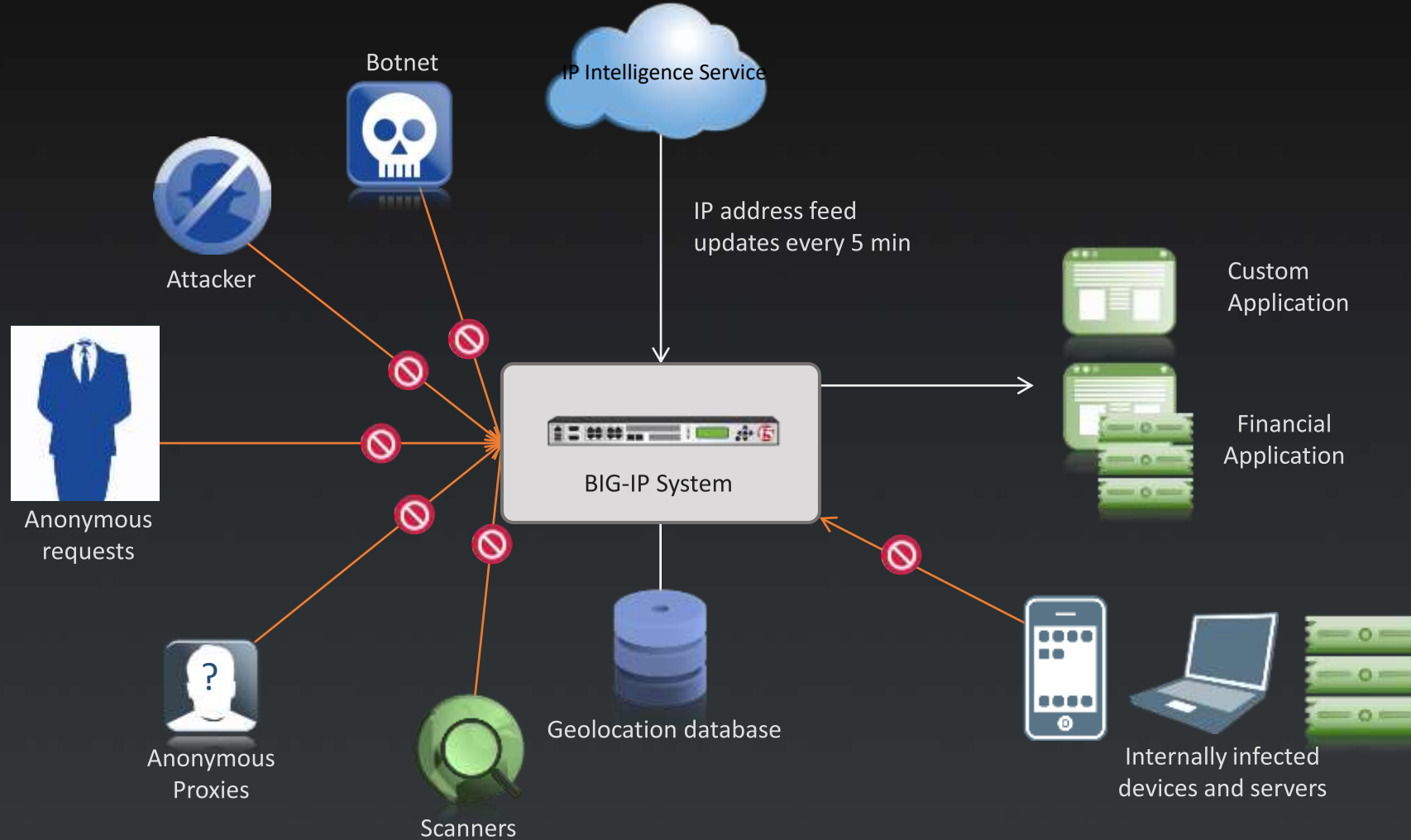
ClickJacking

Business logic flaws



# IP Intelligence

Identify and allow or block IP addresses with malicious activity





# Encryption Creates a Blind Spot in Your Network

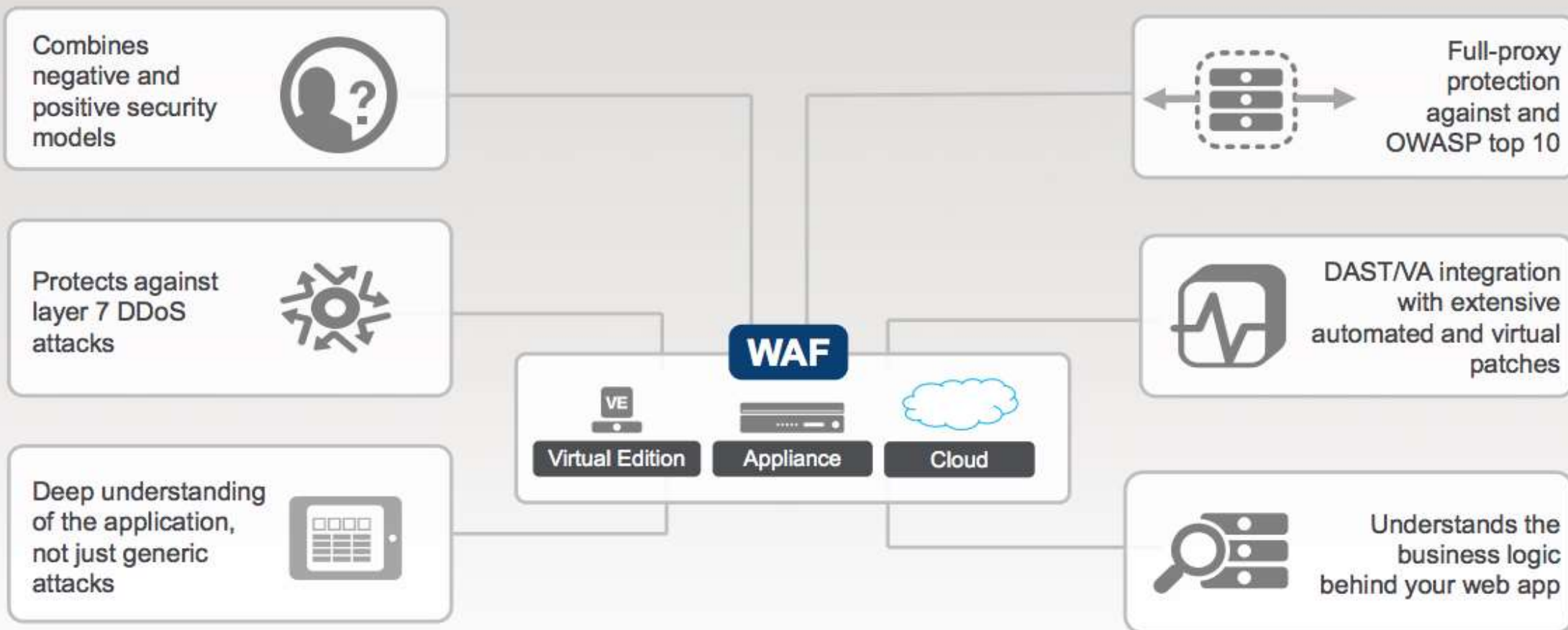
- Most network architectures are not built for SSL encryption
- SSL on NGFW products impacts performance by 80%
- Malware using SSL to evade network monitoring
- Without security tools to inspect SSL traffic, attacker actions can go undetected
- Trends toward SSL Everywhere, including HTTP/2 and TLS 1.3



Cyber criminals are growing  
**more sophisticated** and  
**evasive** in their **attacks**




# Web Application Firewall Capabilities

Protect against layer 7 attacks with granularity



# Traditional Security Devices vs WAF

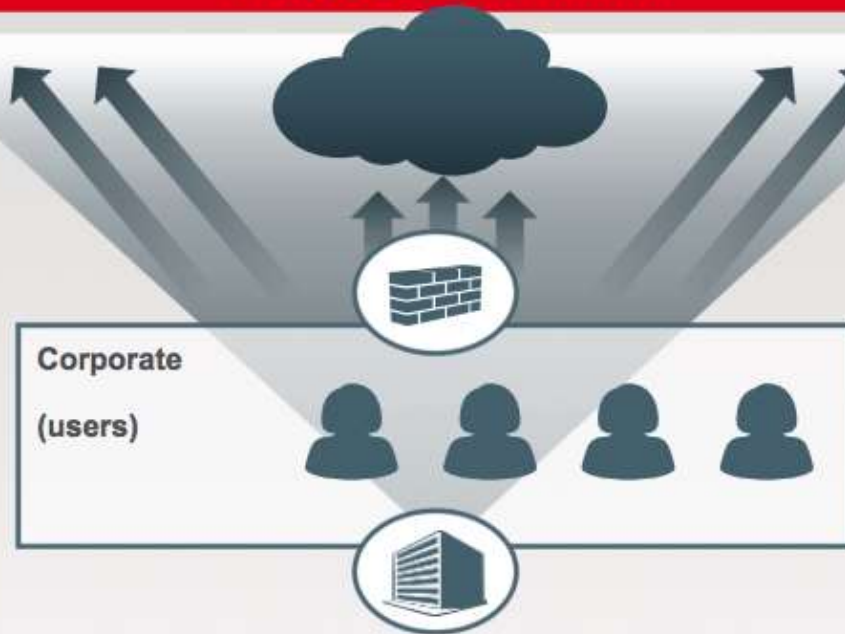
	WAF	IPS	NGFW
Multiprotocol Security *	○	●	●
IP Reputation *	◐	◐	◐
Web Attack Signatures *	●	◐	○
Web Vulnerabilities Signatures *	●	◐	◐
Automatic Policy Learning *	●	○	○
URL, Parameter, Cookie, and Form Protection *	●	○	○
Leverage Vulnerability Scan Results *	●	◐	○
Browser Fingerprinting	●	○	○
Protection against Layer 7 DDoS Attacks	●	○	○
Pro-active Modification of Application Requests/Responses	●	○	○
Advanced Protection for Web Services (SOAP, XML, AJAX)	●	○	○

 = Good to very good  
 = Average or fair  
 = Below average



# The Right Tool for the Job

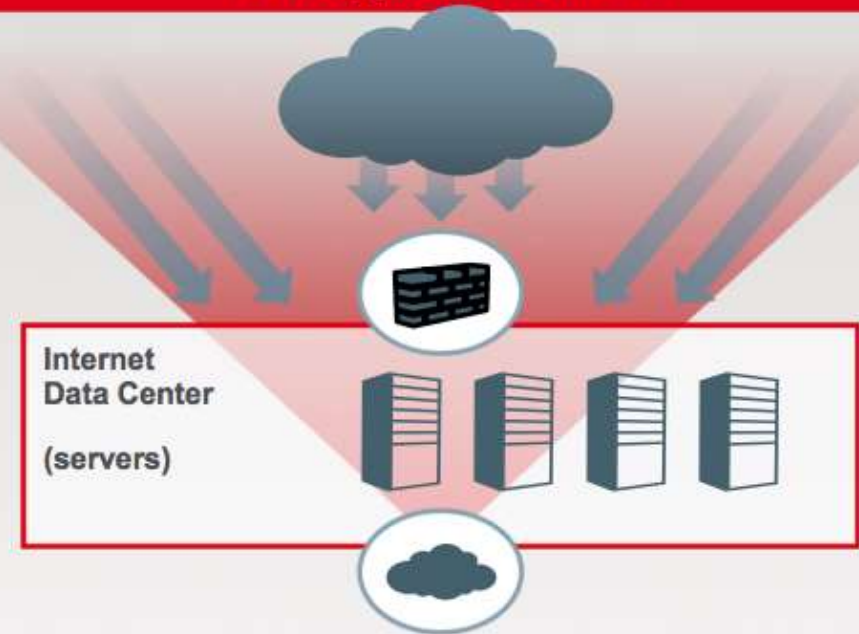
## "Next Generation" Firewall



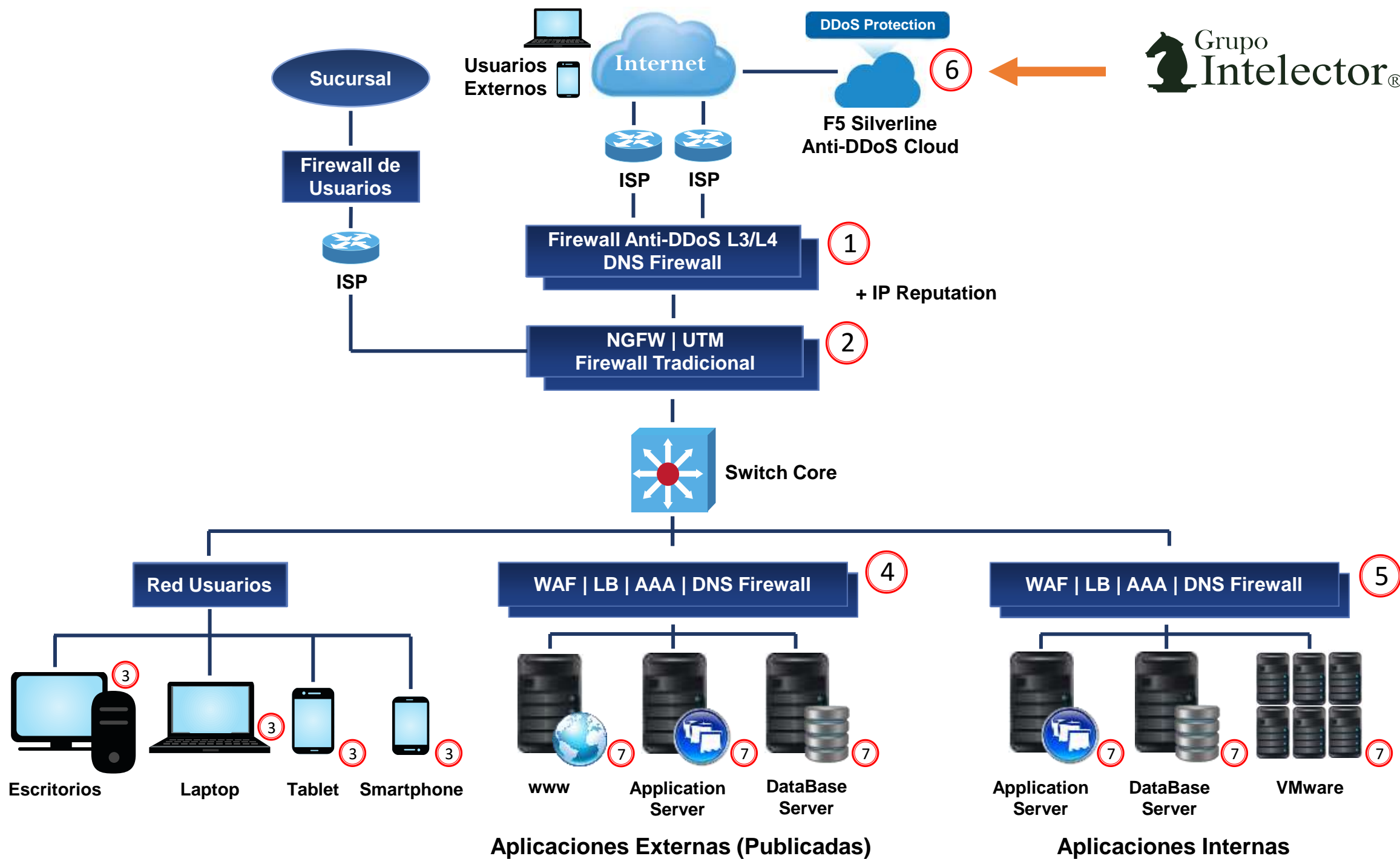
- **Outbound** user inspection
- 1K users to 10K web sites
- Broad but shallow
- UserID and AppID
- Who is doing what?

BIFURCATION OF FIREWALLS

## Web Application Firewall



- **Inbound** application protection
- 1M users to 100 apps
- Narrow but deep
- Application delivery focus
- Web specific protocols (HTTP, SSL, etc.)



# DDoS attacks are easy to launch



... Jmeter, Sc

flooder, PhantomJS

many, many more...

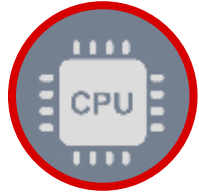


# DDoS Attack Targets



---

Volumetric Attacks on Bandwidth



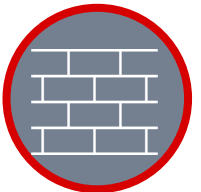
---

Attacks on CPU.  
IPS Signature Scanning.



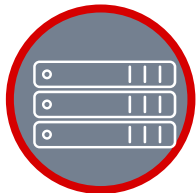
---

Attacks on crypto capacity. SSL floods.



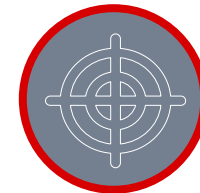
---

Attacks on RAM. Firewall state tables.



---

Attacks on Server stack. Low and Slow.

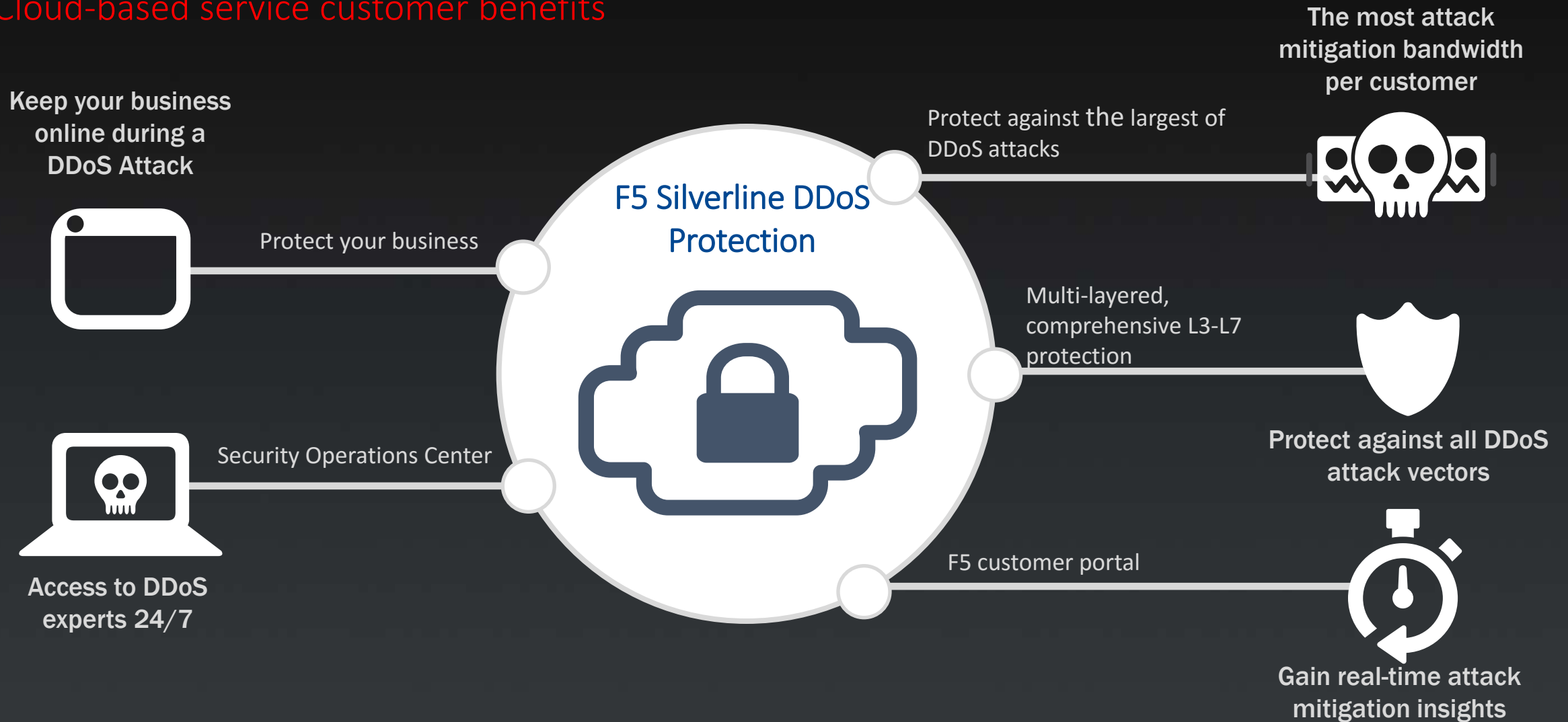


---

Targeted Attacks.  
Bugs and flaws in stack.

# F5 Silverline DDoS Protection

Cloud-based service customer benefits



# Visibility and Reporting



Timeline of events

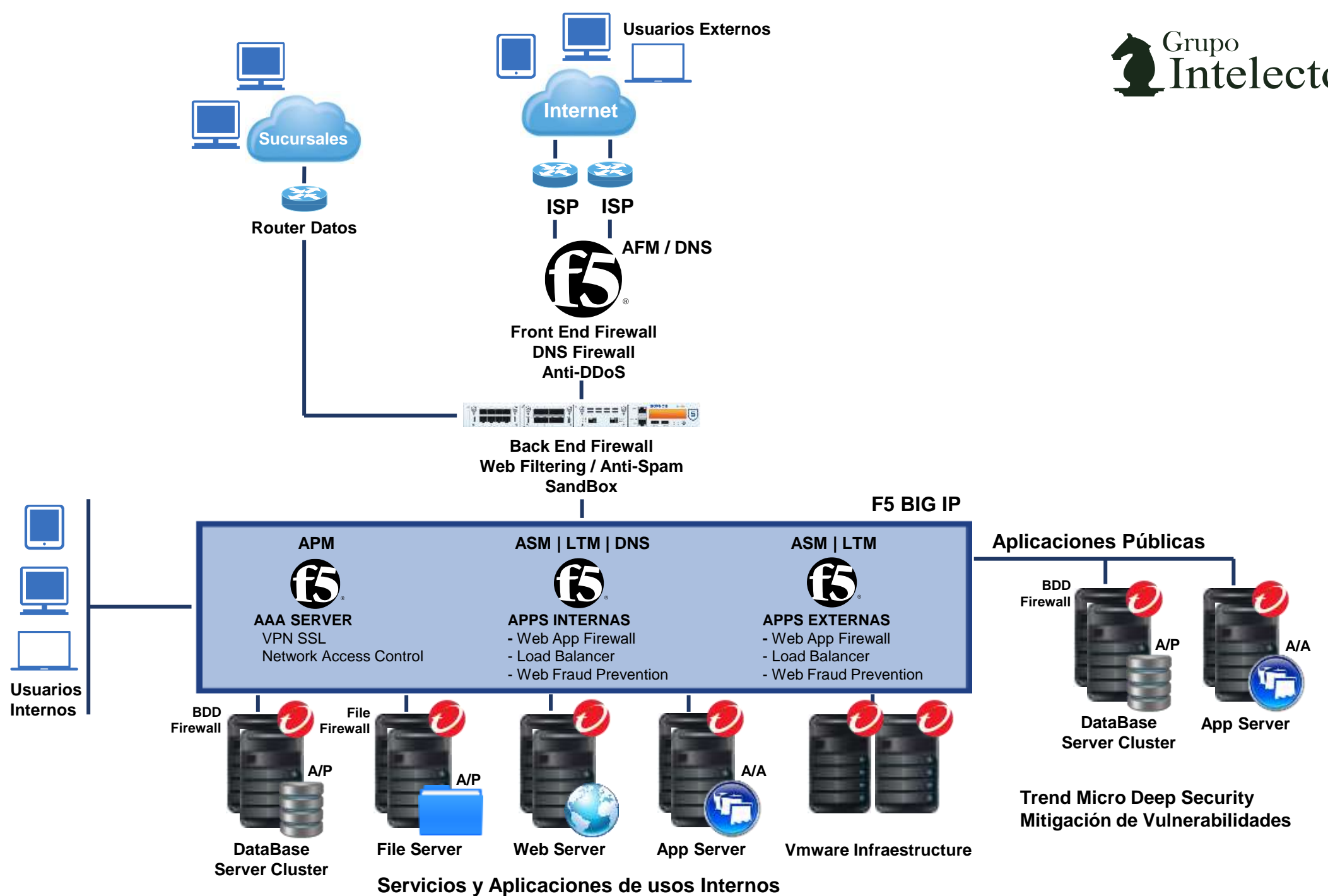
Event Detail

Real time “Attackview” shows:

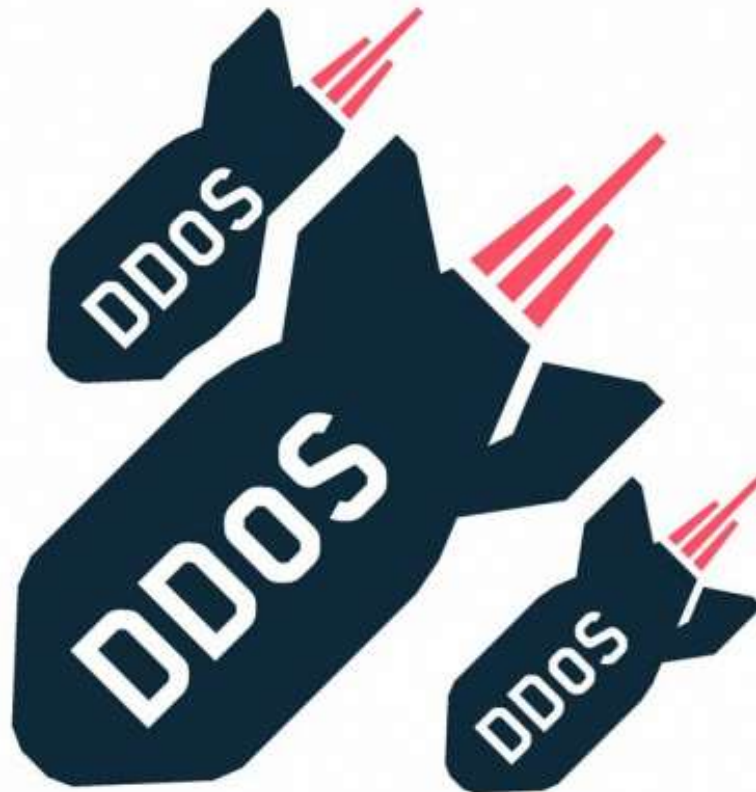
- Type of attack
- IP origin
- Mitigation process
- Yellow flagged annotations of SOC communications







DDoS for Hire | Booters, Stressers, Doosers |  
Attacks are cheap and easy to launch



# Elecciones Presindenciales – Honduras 2017

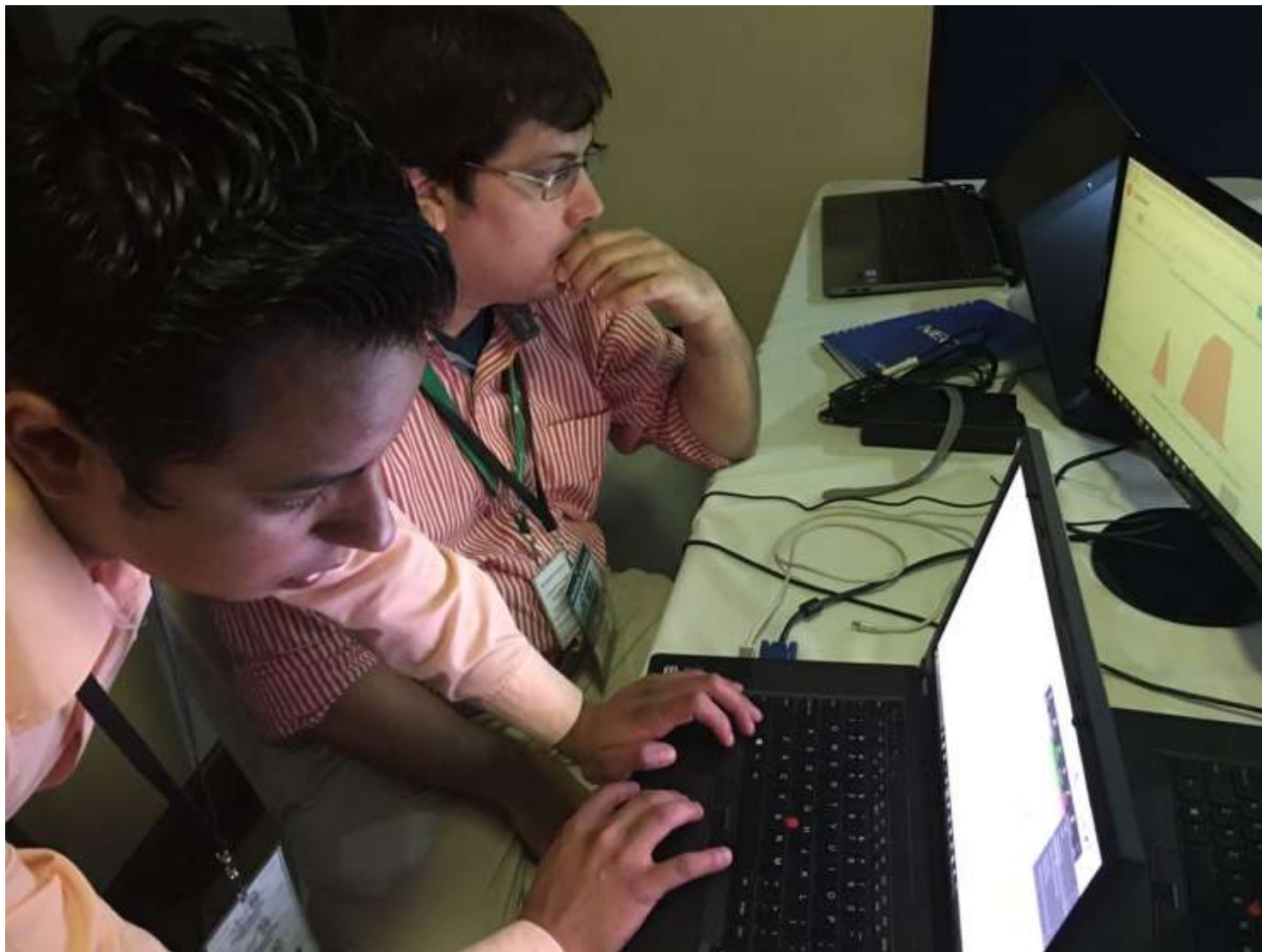




# Elecciones Presindenciales Honduras 2017



# Elecciones Presindenciales Honduras 2017



# Elecciones Presindenciales – Honduras 2017





# Elecciones Presindenciales – Honduras 2017




**¿Es posible cambiar algo que haya entrado ya al sistema?**


"Con los controles que pusimos y las auditorías que están establecidas era imposible. Se hicieron todas las pruebas para que no pudieran “hackearnos” el sistema. Nosotros hemos tenido ataques muy fuertes, empezaron con mayor intensidad a partir del martes después de las elecciones tratando de hacer caer la página web del Tribunal, de esos que se compran el paquete para que bombardee con miles y miles de entradas. Ningún ataque pasó".

# Elecciones Presindenciales Honduras 2017

5 Silverline > My activities

REQUEST #29382 DDOS UDP FLOOD TARGETING 107.162.141.233/32 ~ 729.4 MBPS/85.8 KPPS MITIGATED

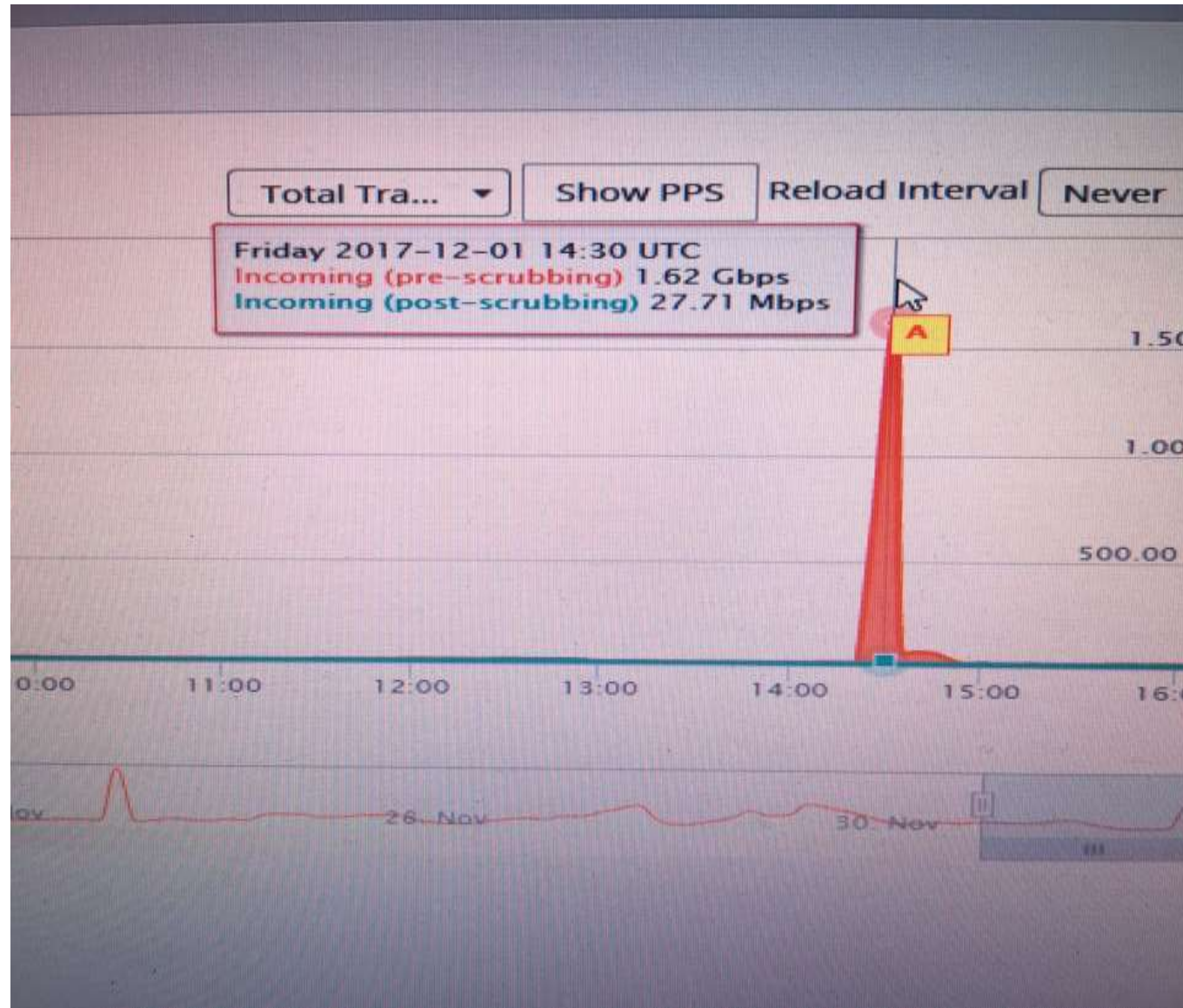
 **Vinoth Elangovan**  
Hello Roger Fonseca, Today at 14:51

 **Alert Number: 1372037** We were notified of a <attack vector> targeting IP 107.162.141.233/32 that reached ~ 729.4 Mbps/85.8 Kpps. Silverline proxy infrastructure is dropping all of attack traffic. Please let us know if there are any questions or concerns.

Thank you,  
Regards,  
Vinoth Elangovan  
F5 Silverline  
Support: (866) 329-4253

Submit

# Elecciones Presindenciales - Honduras 2017





# Top 10 Booter – IP Stresser – IP Booter – Stresser list



# The Top 10 Booter – Ip Stresser – DDoser List

#1 – **iDDos Stresser** – <http://iddos.net>

|500 GBs|Skype Resolver|Stop Button|Unlimited Attacks|Accepts Paypal/Bitcoin|

#2 – **Str3ssed Booter** – <http://str3ssed.me>

|300 GBs|Paypal/Bitcoin|Skype Resolver|Reliable|20Gbps Per Boot|

#3 – **Critical Booter** – <https://www.critical-boot.com>

|90 GBs|Buildable Plans|Accepts Credit Cards|15% Off With Bitcoin|

#4 – **DDos Booter** – <http://ddos.co>

|Very Strong Attacks|Cheap|Nice Interface|Helpful Support|

#5 – **Cloud IP Stresser** – <https://cloudstress.com>

|100 GBs|Cheap|Skype Resolver|

# The Top 10 Booter – Ip Stresser – DDoser List

#6 – **Fiber IP Stresser** – <http://fiberstresser.com>

|Strong Attacks|Cheap|3 Years Running|

#7 – **Net Stresser** – <https://netstress.org>

|40 GBs Per Attack|OVH Drop|Paypal/BTC/PerfectMoney|

#8 – **Power Booter** – <http://powerbooter.net>

|Strong Power|Cheap|

#9 – **Network IP Stresser** – <https://networkstresser.com>

|Cheap|Skype Resolver|

#10 – **Top Booter** – <http://topbooter.com>



# DDoS Demo – Ragebooter.net

## RageBooter

- Dashboard
- PREMIUM FEATURES
  - Attack Hub
  - Attack Scheduling
  - Extras
  - Shoutbox
- OTHER PAGES
  - FAQ
  - ToS
  - Support
  - Downloads
  - Purchase
  - Upgrade

Launch a stress test

Target

Port

Quick Select ▾

Time

0

Method

LDAP (~7 Gbps) ▾

2 - 6

✓

Server

Automatically choose (Recommen

Attack type

Normal ▾

Launch

Server stats (35 server(s) online)

Ping

Name	Attacks	Output	Type	Status
A1	0/1	~10Gbps	Layer 4	Available
A2	0/1	~10Gbps	Layer 4	Available
ALPHA	1/1	~10Gbps	Layer 4	Busy
BRAVO	1/1	~10Gbps	Layer 4	Busy
CHARLIE	1/1	~10Gbps	Layer 4	Busy
DELTA	0/1	~10Gbps	Layer 4	Available

Manage your attacks

What is ?

Clear