BreakingPoint

Powering Accelerated Development

Improving Web Application Firewall Testing (WAF) for better Deployment in Production Networks January 2009 – OWASP Israel

Gregory Fresnais
Director of International Business Development
Email: gfresnais@bpointsys.com, Tel: +33672510922

BreakingPoint Systems

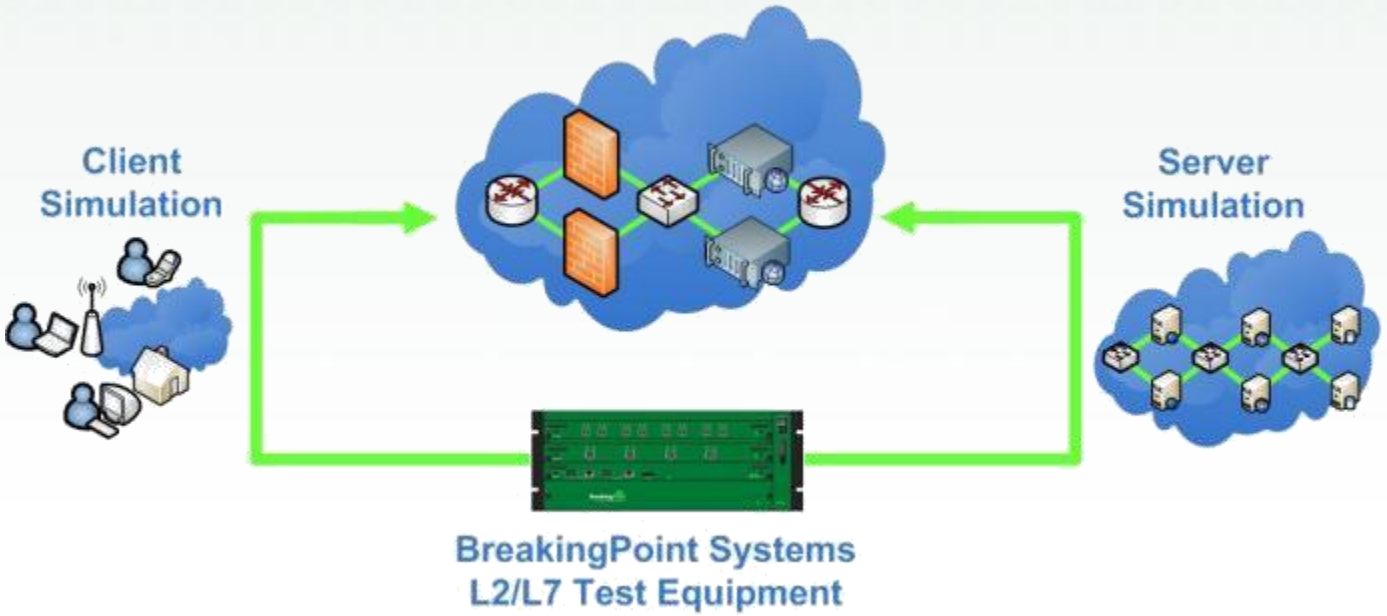
- Founded September 2005
- Management track record

- Deep networking, security, & performance assurance expertise
- Breakthrough, award-winning products

- Privately held and based in Austin, TX
  - Sales & Support: US, Canada, UK, France, Italy, Spain, Netherlands, Belgium, Israel, China, Japan, Korea, Taiwan, Malaysia, New Zeeland, Australia. **Represented by WebHouse Technologies in Israel.**

BreakingPoint
Powering Accelerated Development

What Does BreakingPoint Deliver?



- Comprehensive Layer 2-7 testing for network equipment and application servers
- High-performance, compact, flexible and easy-to-use products
- Realistic performance and security validation using stateful application protocols and live security attacks

Examples of BreakingPoint Tests

Realistic Traffic Emulation: Layer 2-7

Bit Blaster - Generates Ethernet frames (L2 Tests)

Routing Robot - Generates IP packets (L3 Tests)

Session Sender - Generates valid TCP sessions (L4 Tests)

App Sim – Generates 70+ realistic application flows (L7 Tests)

Capture and Recreate - Capture and playback PCAP

Malicious Traffic Simulation Layer 2-7

Security Module – 3,700+ unique attacks, 80+ evasion types

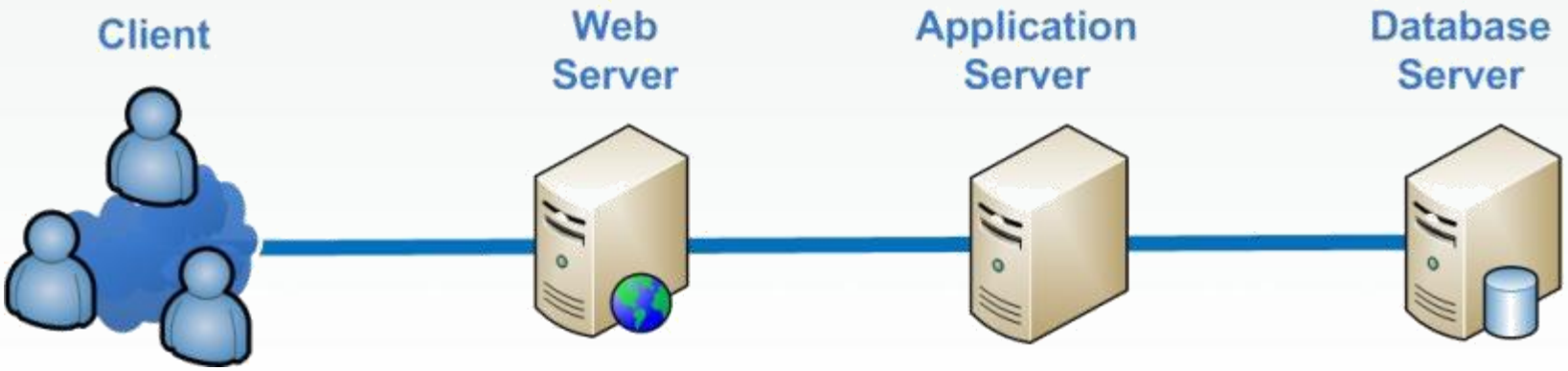
Stack Scrambler – Protocol fuzzing

70+ Client and Server Protocols Supported

- HTTP
- HTTPS
- POP3
- IMAP
- Finger
- RTMP
- MAPI
- Yahoo! Messenger
- Informix Database
- MSN Messenger
- Jabber ICQ
- QOTD
- Gopher
- DNS
- RTP
- SIP TCP/UDP
- SMTP
- RTSP
- SNMP
- FTP
- RLogin
- Rshell
- QQ Messenger
- RSync
- DB2 Database
- AOL IM
- BOOTPS
- DCE/RPC
- LDAP
- NFSD
- NTP
- SSH
- Postgres Database
- FIX
- FIXT
- CIFS SMB
- BitTorrent
- eDonkey
- NetBIOS
- RADIUS Accounting
- RADIUS Access
- Gnutella
- VMware VMotion
- Telnet
- Sybase Database
- MM4
- Oracle Database
- Microsoft SQL Server
- World of Warcraft
- …

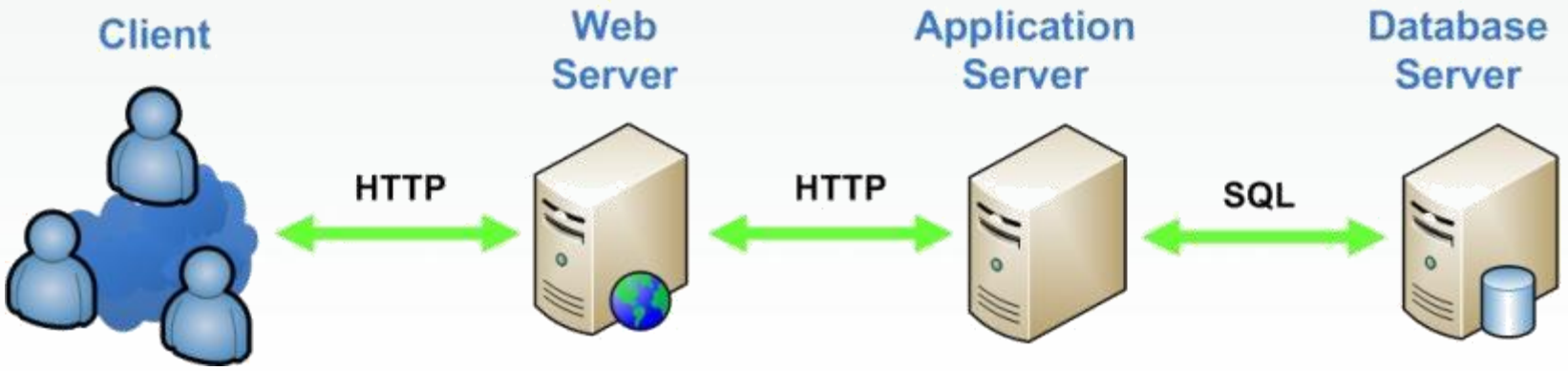
Web Application Firewall Deployment Scenarios

Simple Web Service Infrastructure



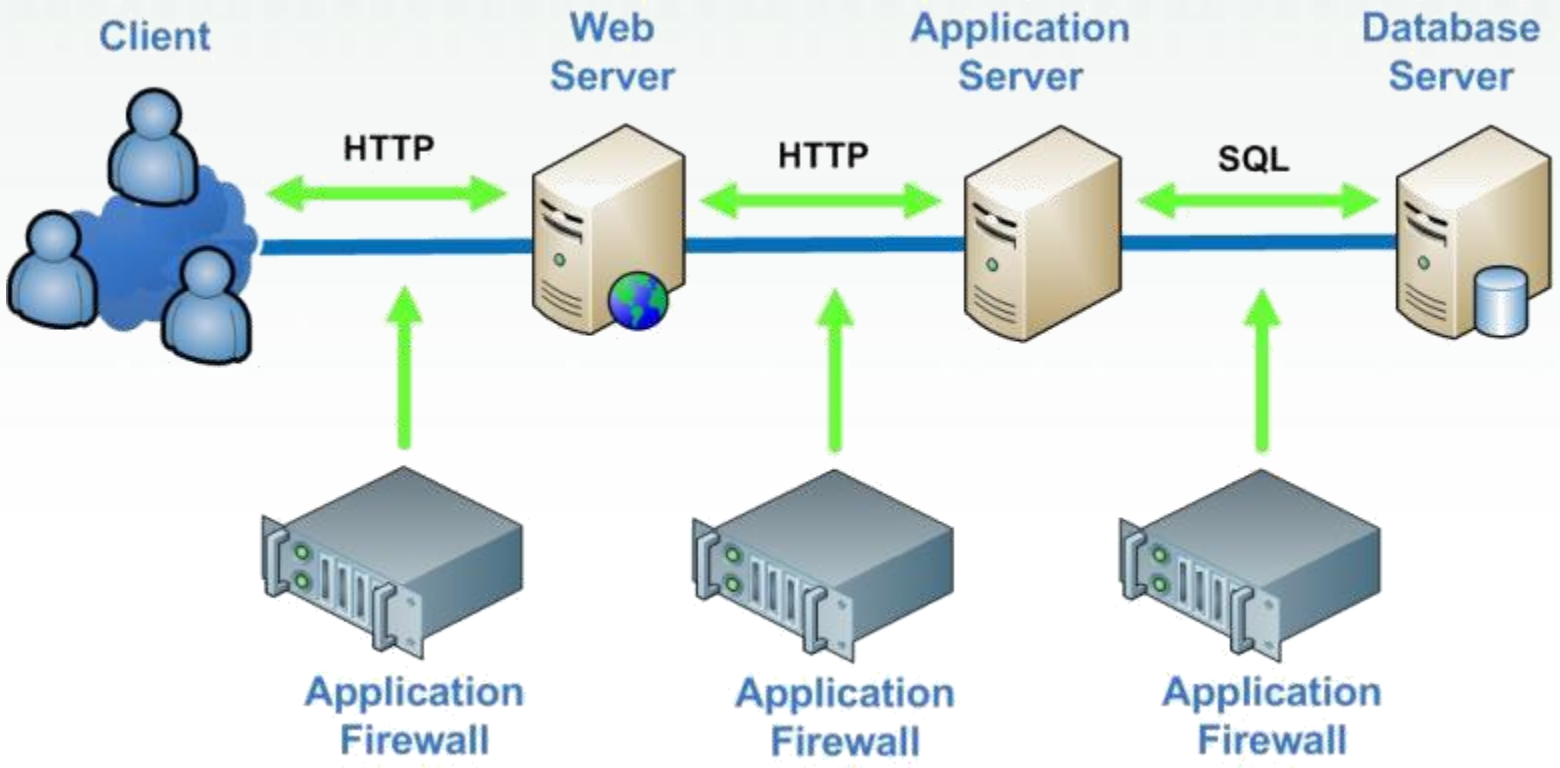
- Topology:
  - Client
  - Web Server
  - Application Server
  - Database Server

Different Protocols to Exchange Information



- Communication between Client and Web Server over HTTP
- Communication between Web and Application Servers over HTTP
- Communication between Application and Database Server over SQL

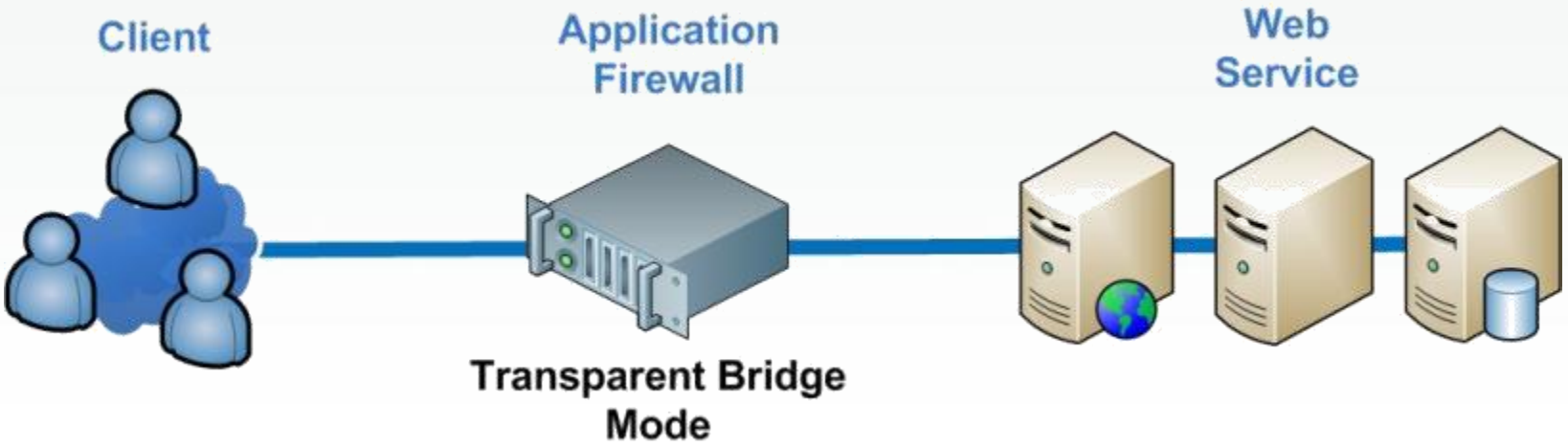
Different Types of WAF



- Deploy WAFs between Client and Server, Web Server and Application Server, and Application Server and Database Server

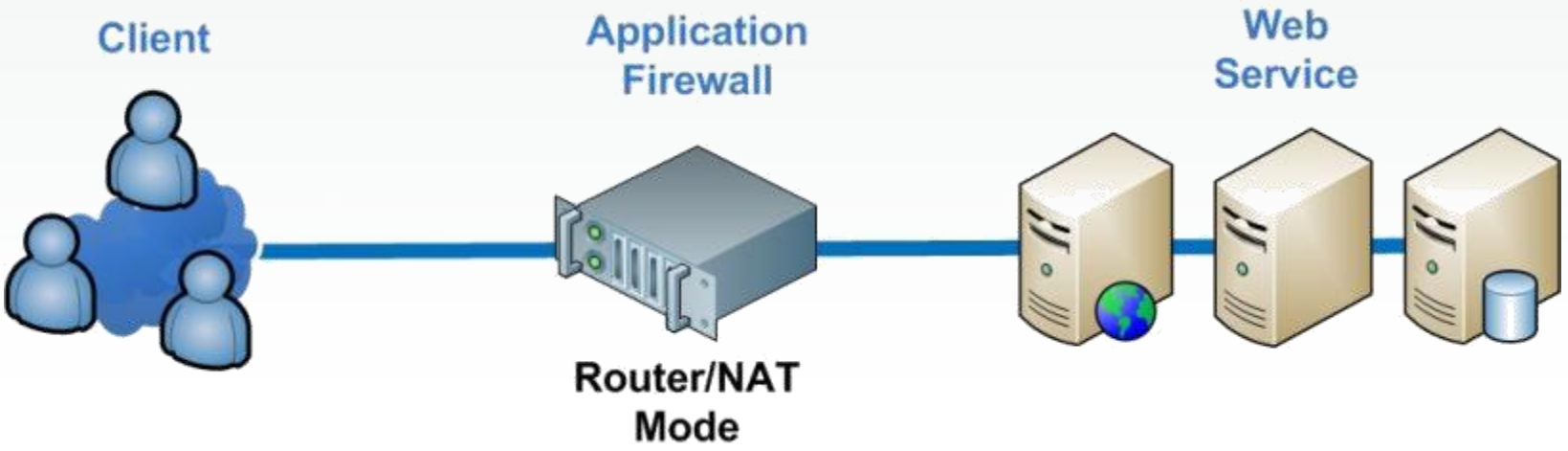
Network Topologies for Deploying Web Application Firewall

Transparent Bridge Deployment



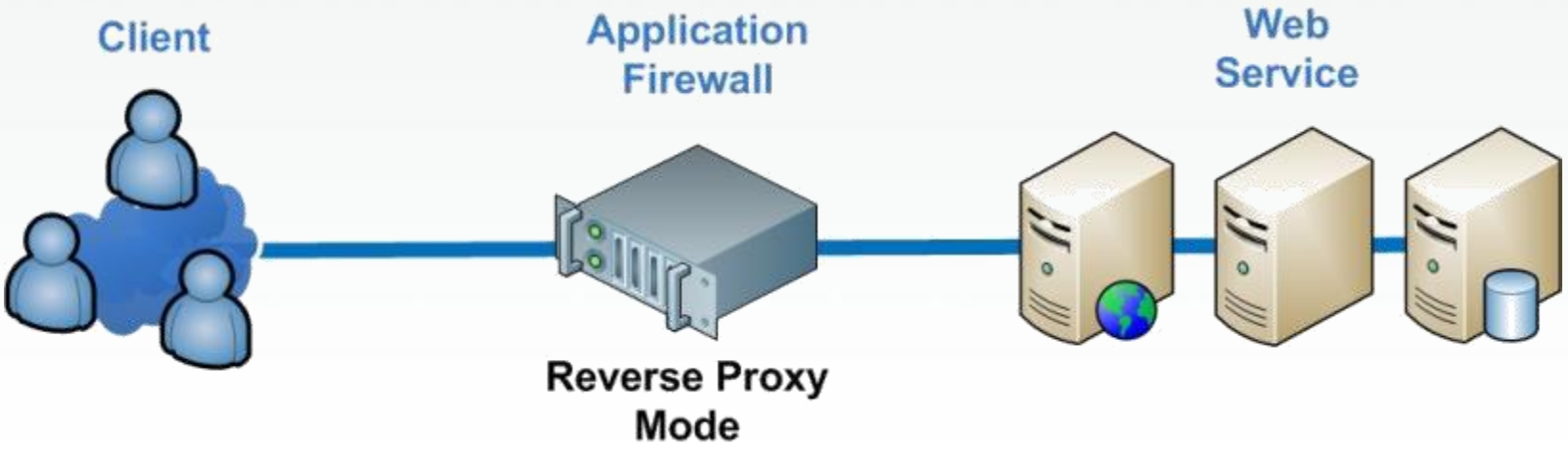
- WAF deployed in Transparent Bridge
- Client and Server in same subnet

Router/NAT Deployment



- WAF deployed in Router/NAT
- Client and Server in different subnet
- Server IP address abstracted

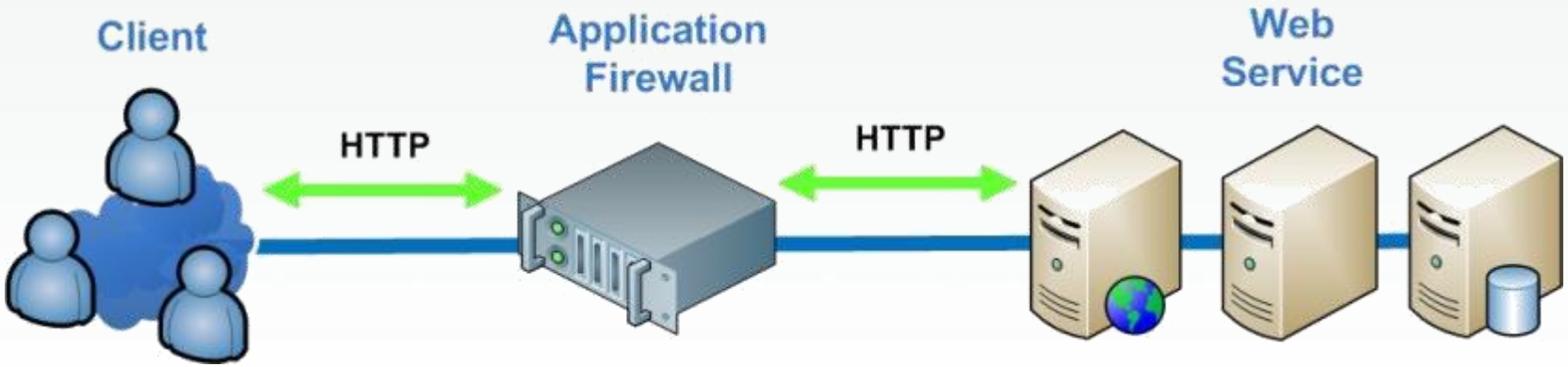
Reverse Proxy Deployment



- WAF deployed in Reverse Proxy
- Client and Server in different subnet
- Server IP address abstracted
- L7 features enabled like Load Balancing, Compression, Caching, TCP Connection Multiplexing, URL Rewriting, etc …

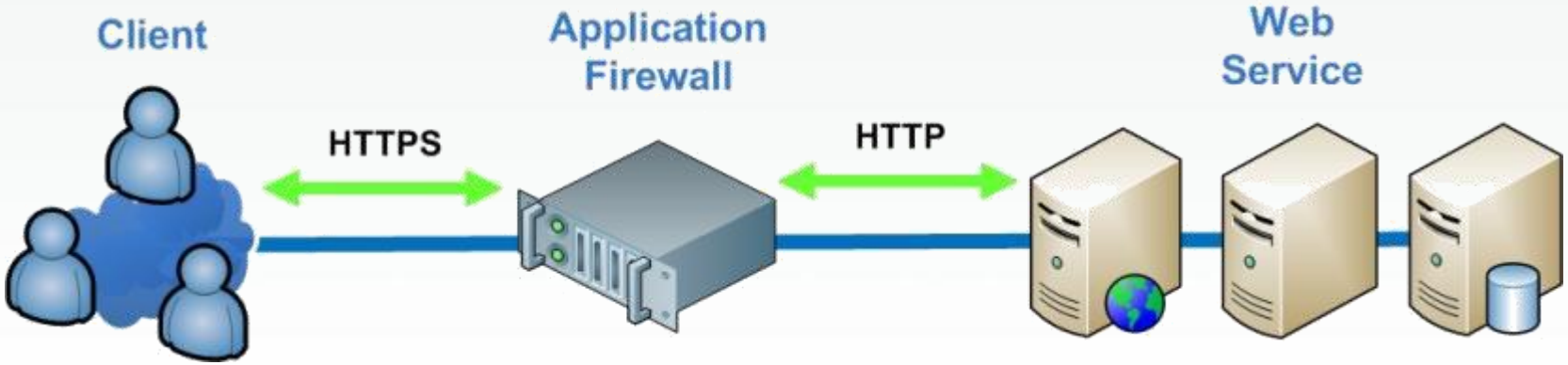
Configuration Options for Deploying Web Application Firewall

Communication Via HTTP



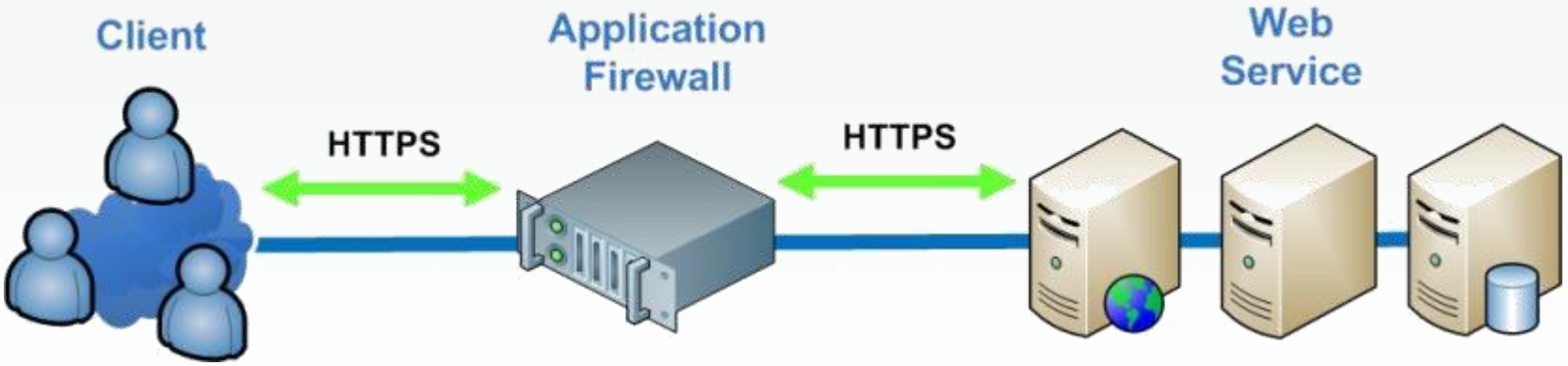
- Communication between the Client and the WAF over HTTP
- Communication between the WAF and the Server over HTTP

Communication Via HTTPS and HTTP



- Communication between the Client and the WAF over HTTPS
- Communication between the WAF and the Server over HTTP

Communication Via HTTPS



- Communication between the Client and the WAF over HTTPS
- Communication between the WAF and the Server over HTTPS

Communication Via SQL

- Communication between the Client and the WAF over SQL
- Communication between the WAF and the Server over SQL

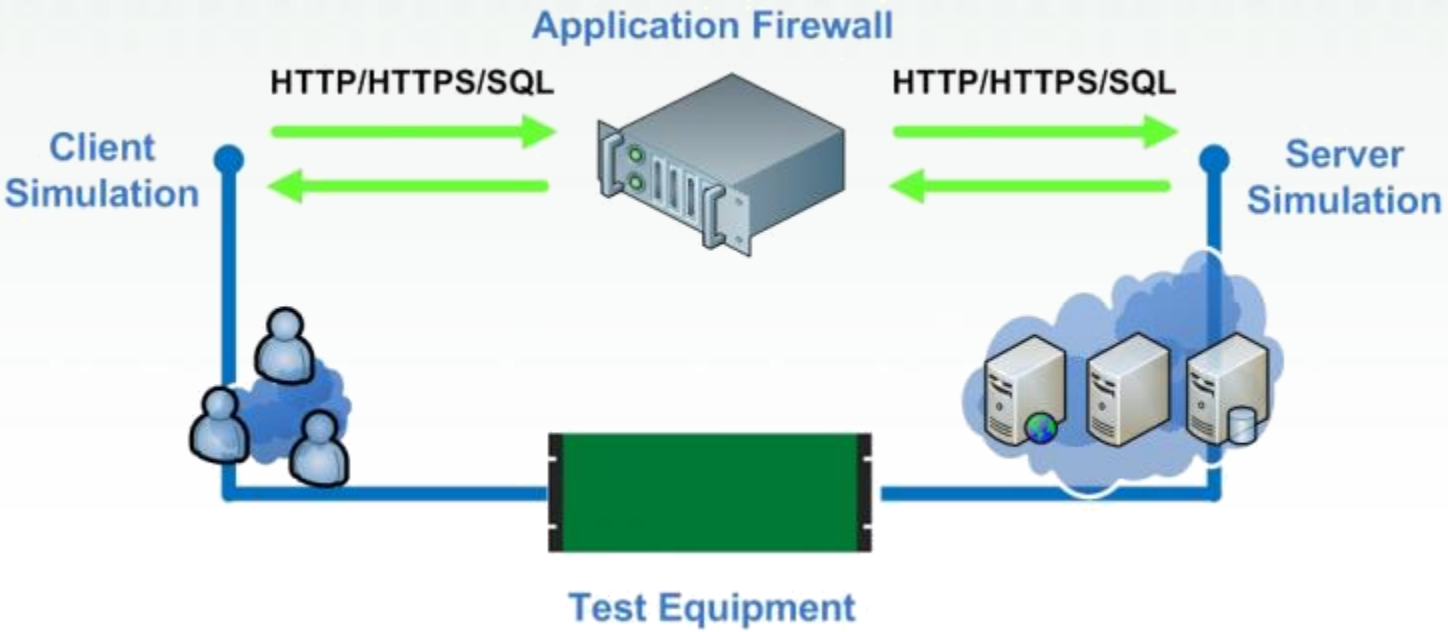
Testing Web Application Firewalls Before Deployment

WAF Vendor Comparison

- Cannot make the right decision with the limited information on vendor datasheets
- What are the HTTP Transactions per Second?
  - HTTP 1.0 vs. HTTP 1.1, Object Size, TCP Close RST vs. FIN, …
- What are the HTTPS Transaction per Second?
  - HTTP 1.0 vs. HTTP 1.1, Object Size, Key Size, Cipher, SSL Re-use ID, …
- What is the HTTPS Bandwidth?
  - HTTP 1.0 vs. HTTP 1.1, Object Size. Key Size, Cipher, SSL Re-use ID, …

Testing
Web Application Firewalls

Web Application Firewall Testing Infrastructure



Test Equipment Capabilities:

- Simulate a large number of different Clients and Servers
- Simulate different application protocols and define a variety of settings to validate the WAF under different configurations
- Reach the limitation of WAF

Types of Tests Required to Validate Web Application Firewalls

Lab Test Scenario – WAF Test Methodology

- Test executed on several Web Application Vendor products
- Web Application Firewall Performance with Good Traffic
  - Maximum HTTP Transaction per Second
  - Maximum SQL Queries per Second
  - Maximum Concurrent TCP Connections
  - Maximum HTTP Bandwidth
  - Maximum SQL Bandwidth
- Web Application Firewall Performance with Security Attacks
  - Maximum HTTP Attacks per Second
  - Maximum SQL Attacks per Second
- Web Application Firewall Performance Blended Traffic
  - Maximum HTTP Transaction per Second with Attacks
  - Maximum SQL Queries per Second with Attacks

Real-World Test Scenario - WAF Test Methodology

- Test executed on one Web Application Vendor product
- Web Service Performance Without the Web Application Firewall
  - Maximum New Users per Second
  - Maximum Concurrent Users
  - Maximum Bandwidth
- Web Service Performance With the Web Application Firewall
  - Maximum New Users per Second
  - Maximum Concurrent Users
  - Maximum Bandwidth
- Web Service Security with Web Application Firewall
  - Mix Good Traffic and Security Attacks

Maximum
WAF Performance
“Lab Test Scenario”

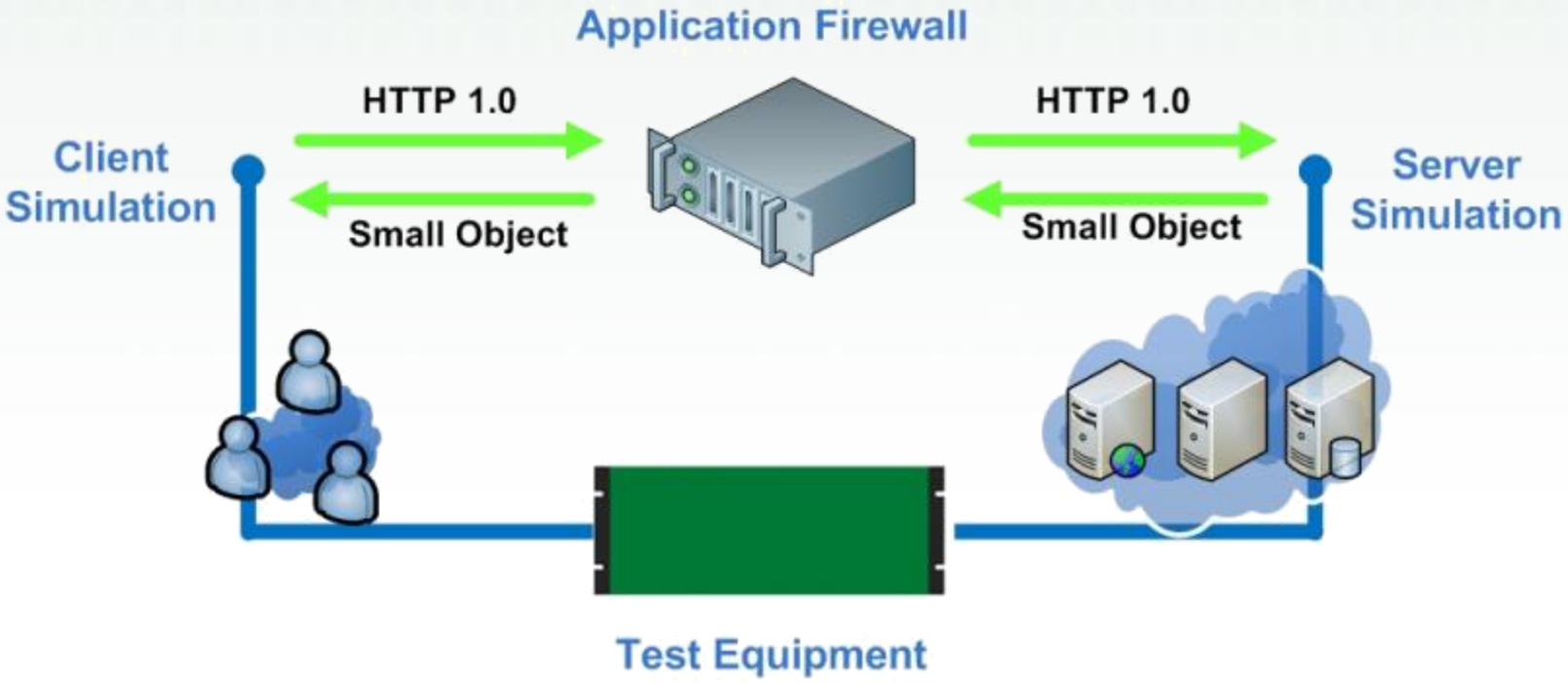
Web Application Firewall Performance for "Good Traffic"

Maximum HTTP Transactions per Second Supported by WAF "Worst Case"

Maximum HTTP 1.0 Transactions per Second

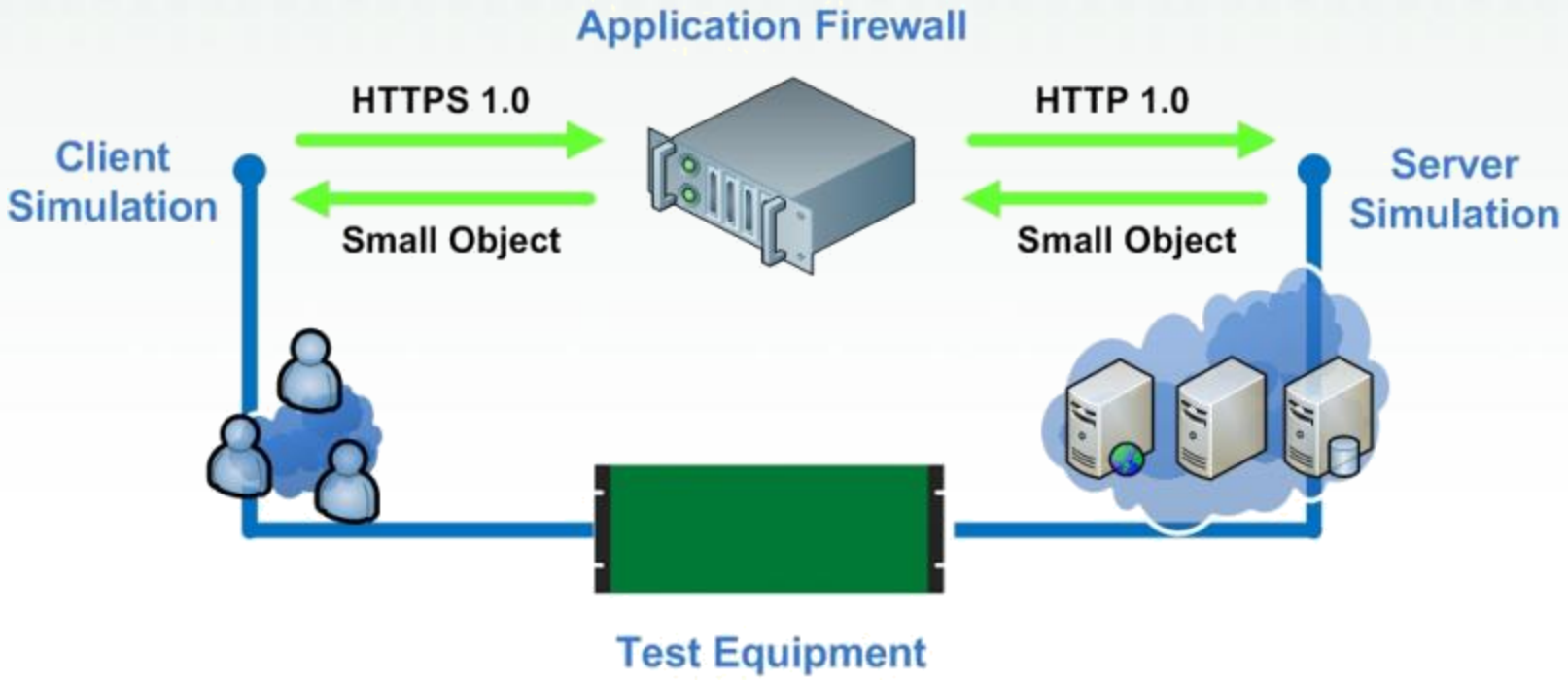
- Test Objective
  - Find the Maximum HTTP Transactions per Second in worst case where 1 HTTP transaction is sent over one TCP Connection.
- Breaking Point
  - Low HTTP Transaction Response Time
  - Low Number of Concurrent TCP Connections
  - 100% of HTTP Transaction Successful
- Performance Measurement
  - Maximum HTTP Transaction per Second
  - Average HTTP Transaction Response Time
  - Maximum Concurrent TCP Connections
  - Bandwidth

Communication Via HTTP



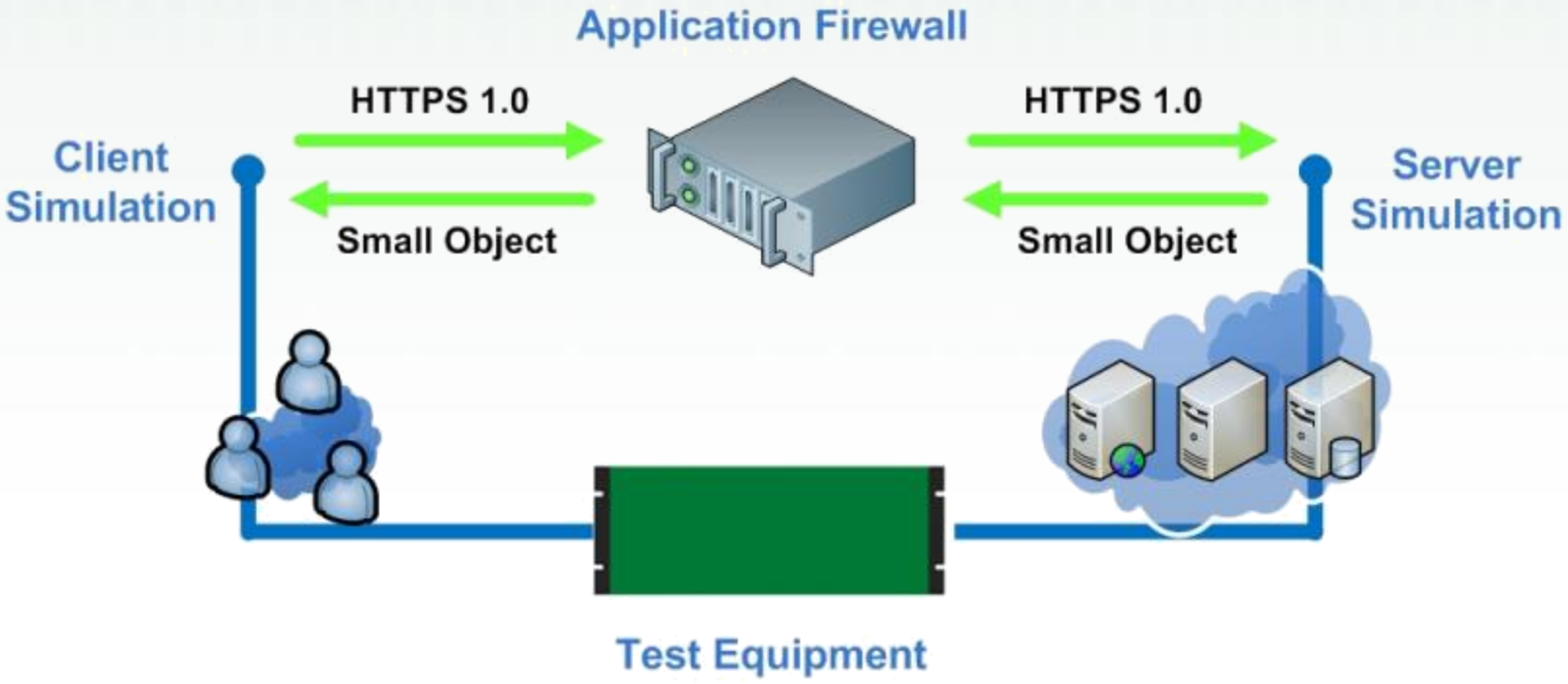
- Check performance using different Oobject sizes: 1024, 5120, 10240 and 51200

Communication Via HTTPS and HTTP



- Check performance using different object size
- Check performance using different key size: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Communication Via HTTPS



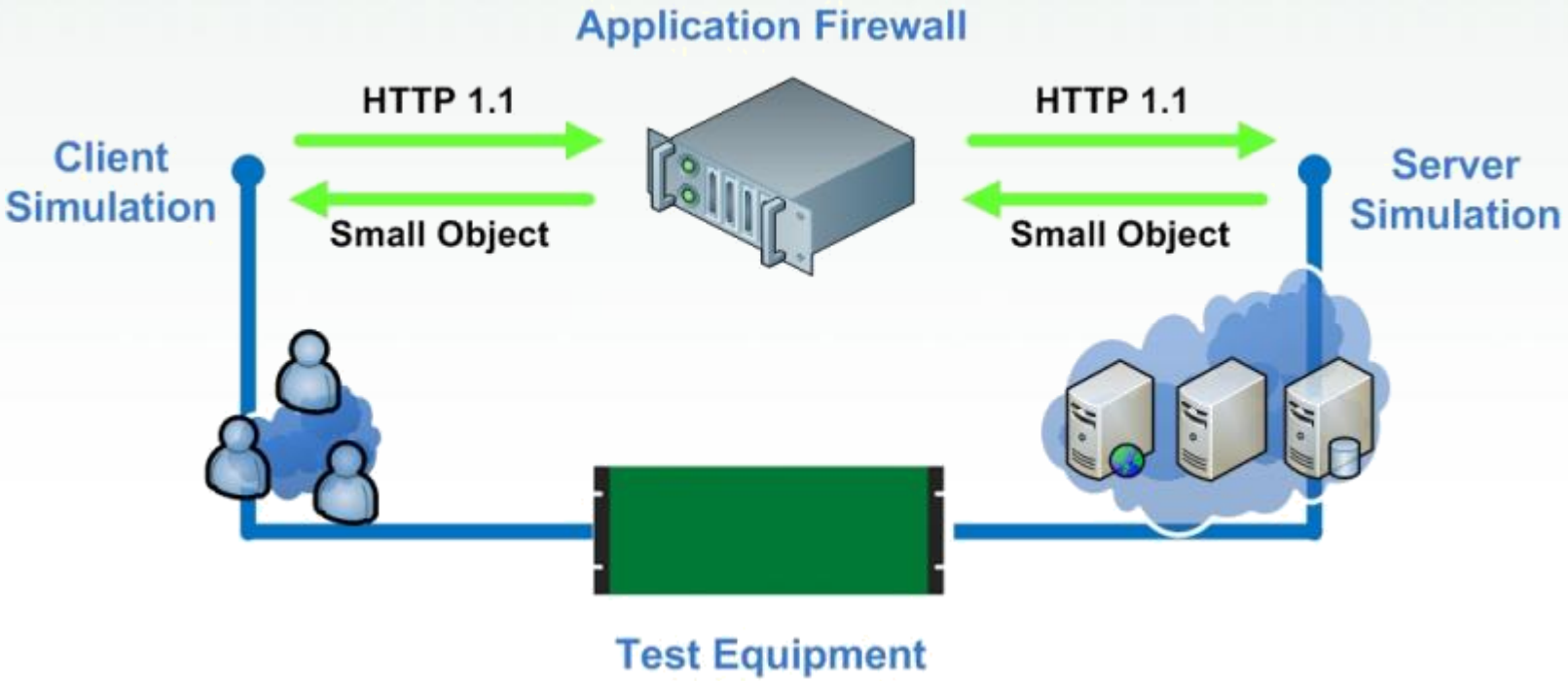
- Check performance using different object size
- Check performance using different key size: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Maximum HTTP Transactions per Second Supported by WAF "Best Case"

Maximum HTTP 1.1 Transaction per Second

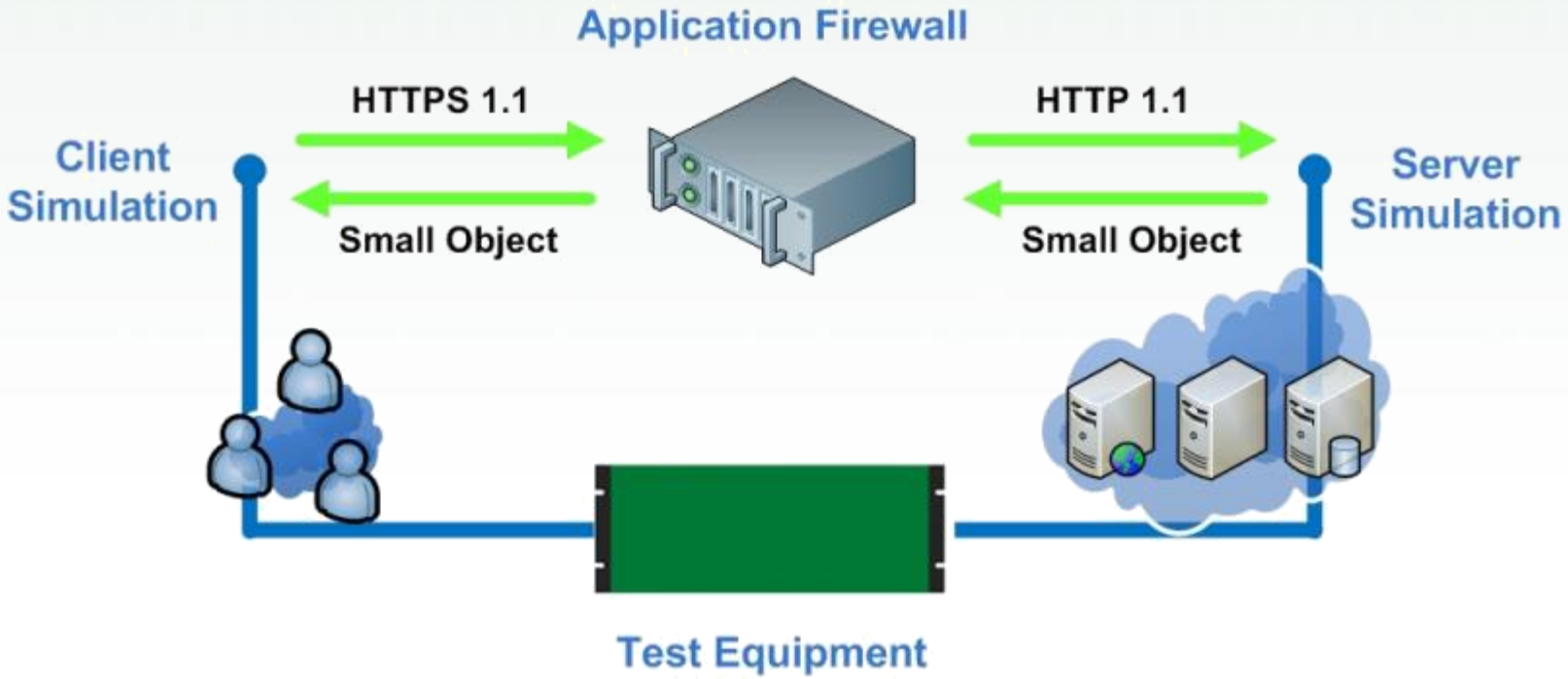
- Test Objective
  - Find the Maximum HTTP Transactions per Second in best case where several HTTP transactions are sent over 1 TCP Connection.
- Breaking Point
  - Low HTTP Transaction Response Time
  - Low Number of Concurrent TCP Connections
  - 100% of HTTP Transaction Successful
- Performance Measurement
  - Maximum HTTP Transaction per Second
  - Average HTTP Transaction Response Time
  - Maximum Concurrent TCP Connections
  - Bandwidth

Communication Via HTTP



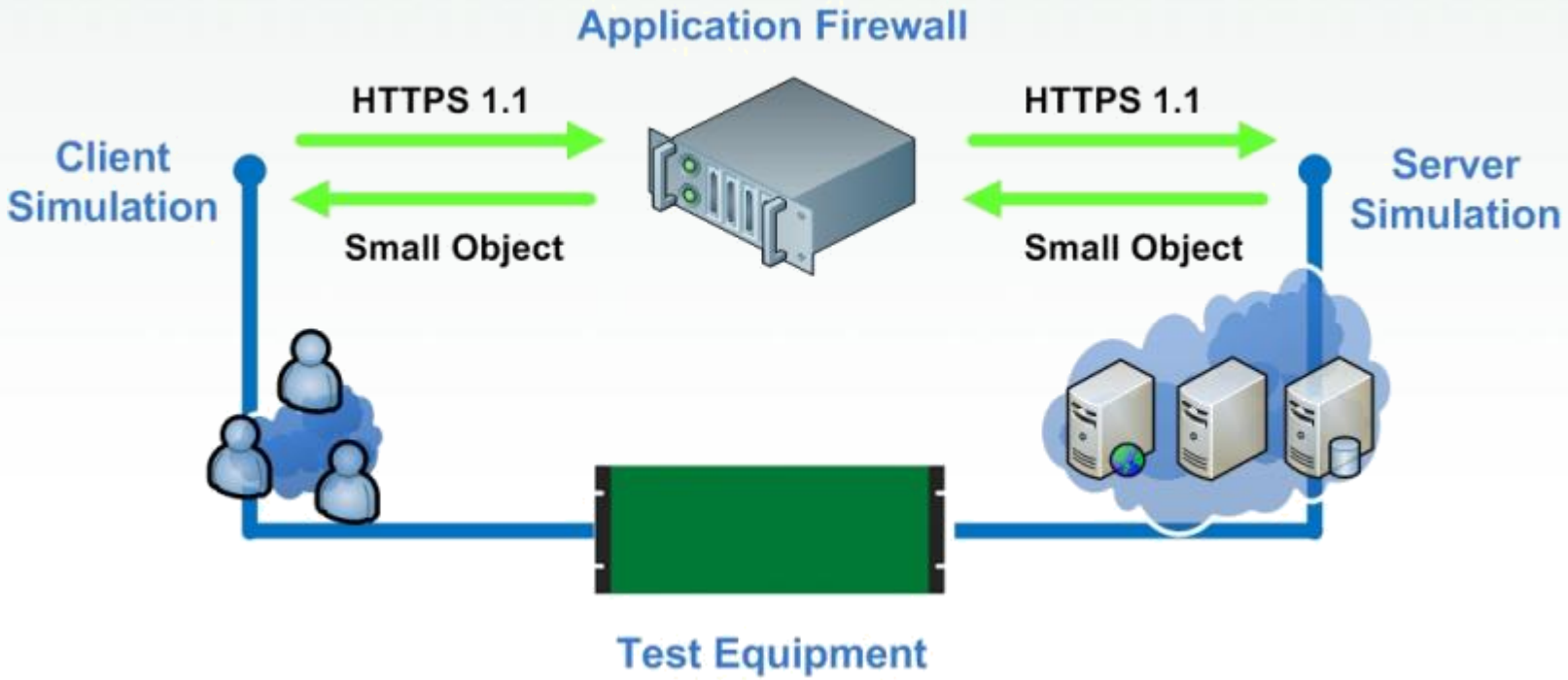
- Check performance using different object sizes: 1024, 5120, 10240 and 51200

Communication Via HTTPS and HTTP



- Check performance using different object sizes
- Check performance using different key sizes: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Communication Via HTTPS



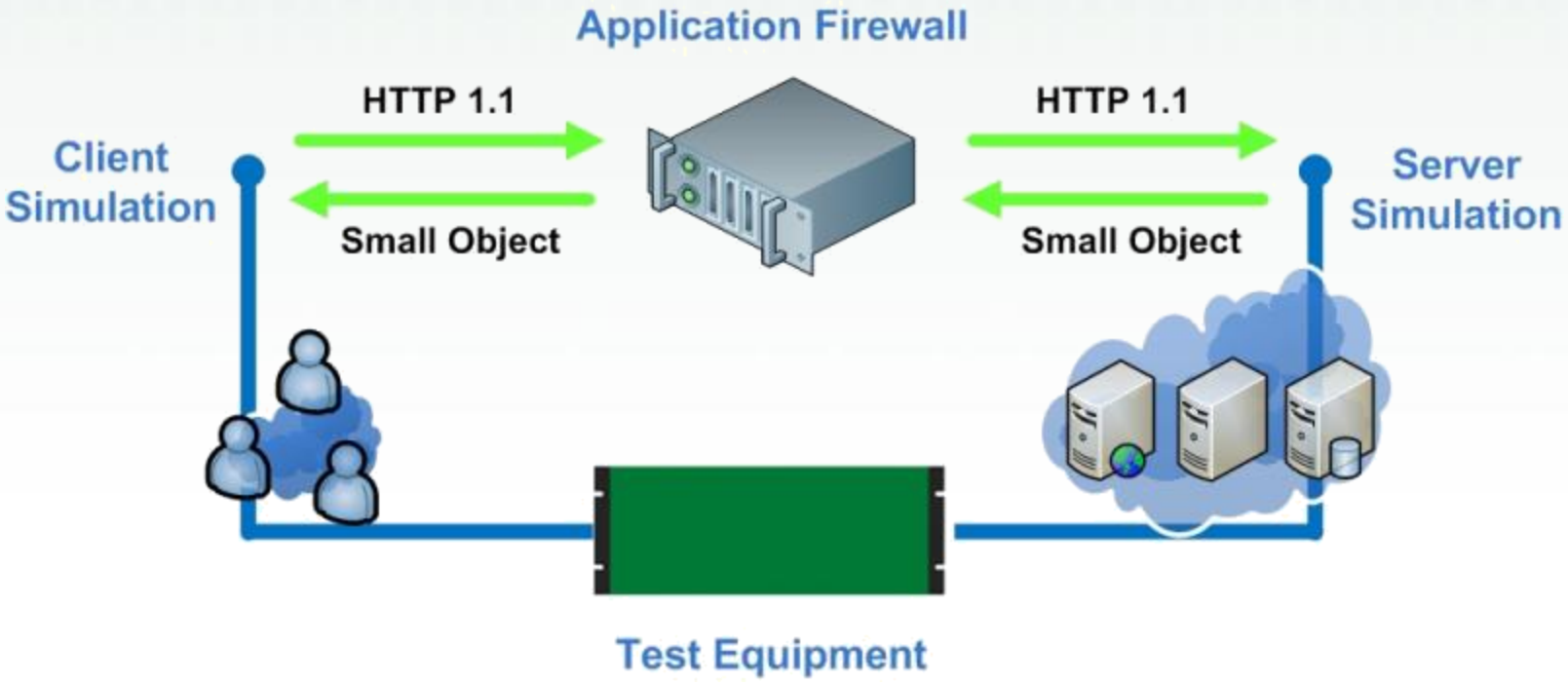
- Check performance using different object Sizes
- Check performance using different key sizes: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Maximum Concurrent TCP Connections Supported by WAF

Maximum Concurrent TCP Connections

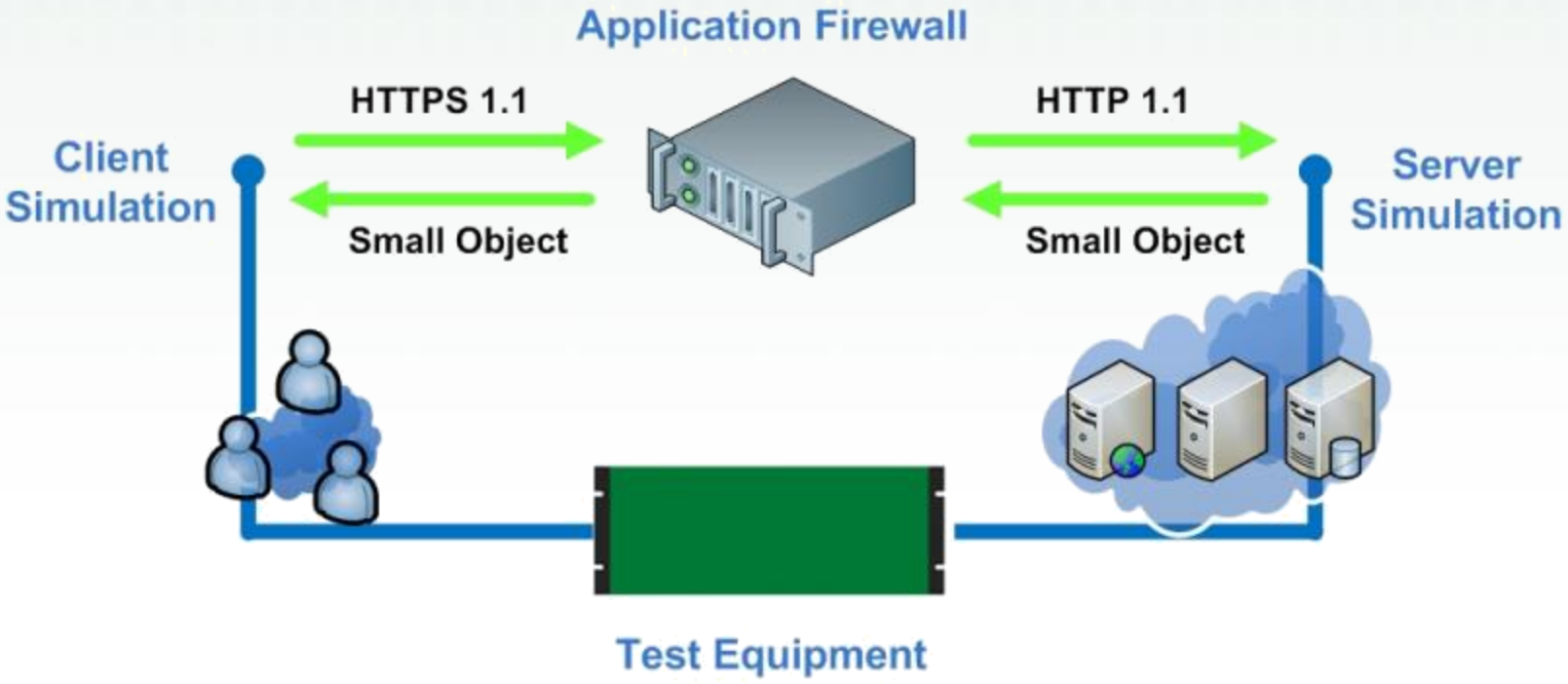
- Test Objective
  - Find the maximum concurrent TCP connections where several HTTP transactions are sent over one TCP connection.
  - Client Think Time is inserted between each client request to keep the TCP connection open.
- Breaking Point
  - Low HTTP Transaction Response Time
  - 100% of HTTP Transaction Successful
- Performance Measurement
  - Maximum Concurrent TCP Connections
  - Maximum HTTP Transaction per Second
  - Average HTTP Transaction Response Time
  - Bandwidth

Communication Via HTTP



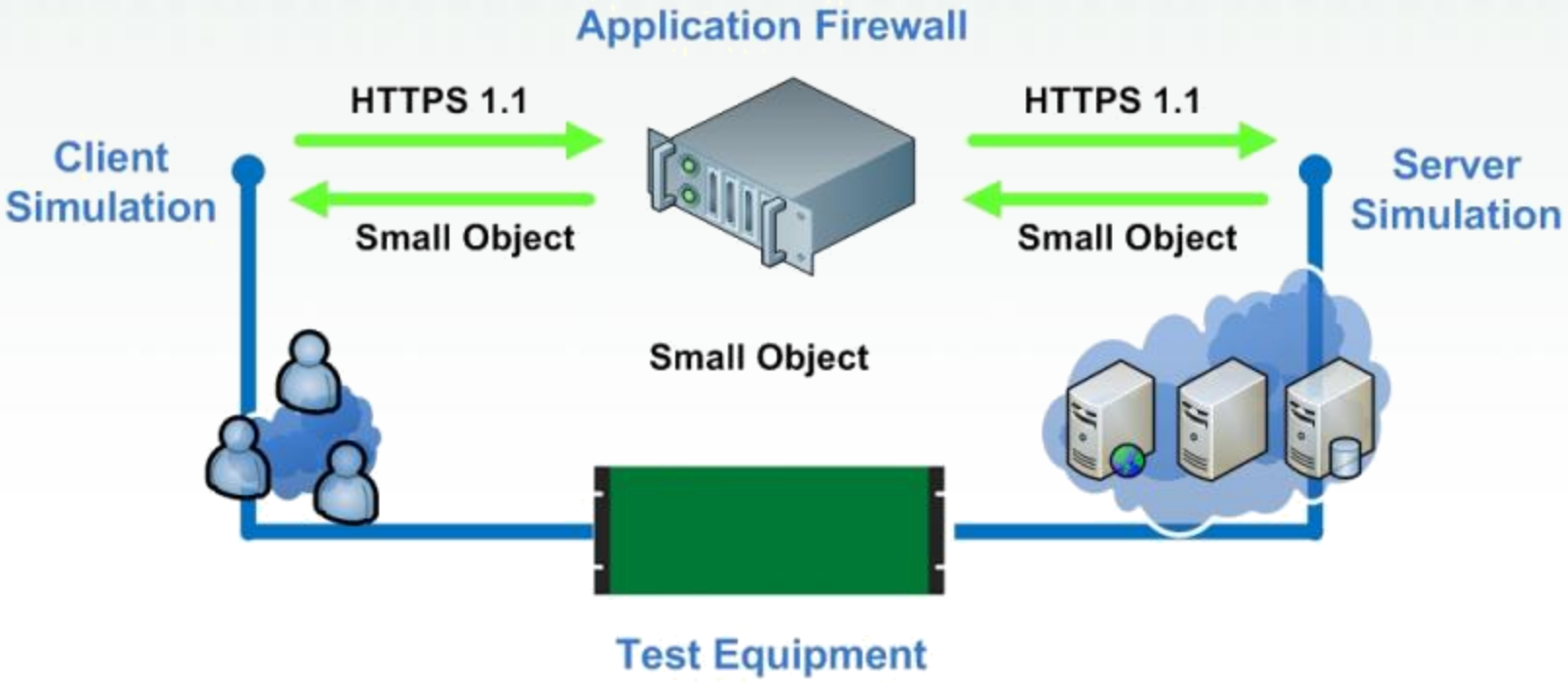
- Check performance using different small object sizes: 1024

Communication Via HTTPS



- Check performance using different object sizes: 1024
- Check performance using different key sizes: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Communication Via HTTPS



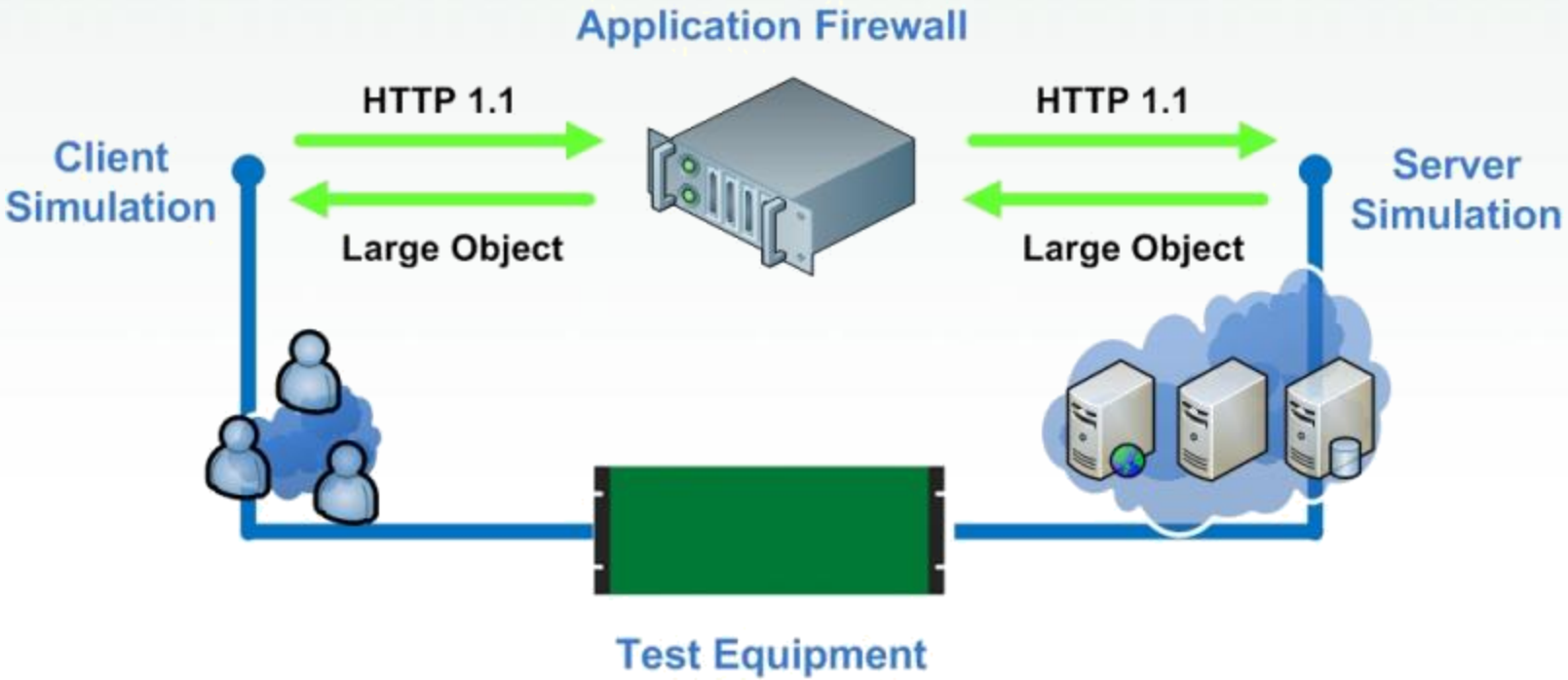
- Check performance using different object sizes: 1024
- Check performance using different key sizes: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Maximum HTTP Bandwidth Supported by WAF

Maximum HTTP Bandwidth

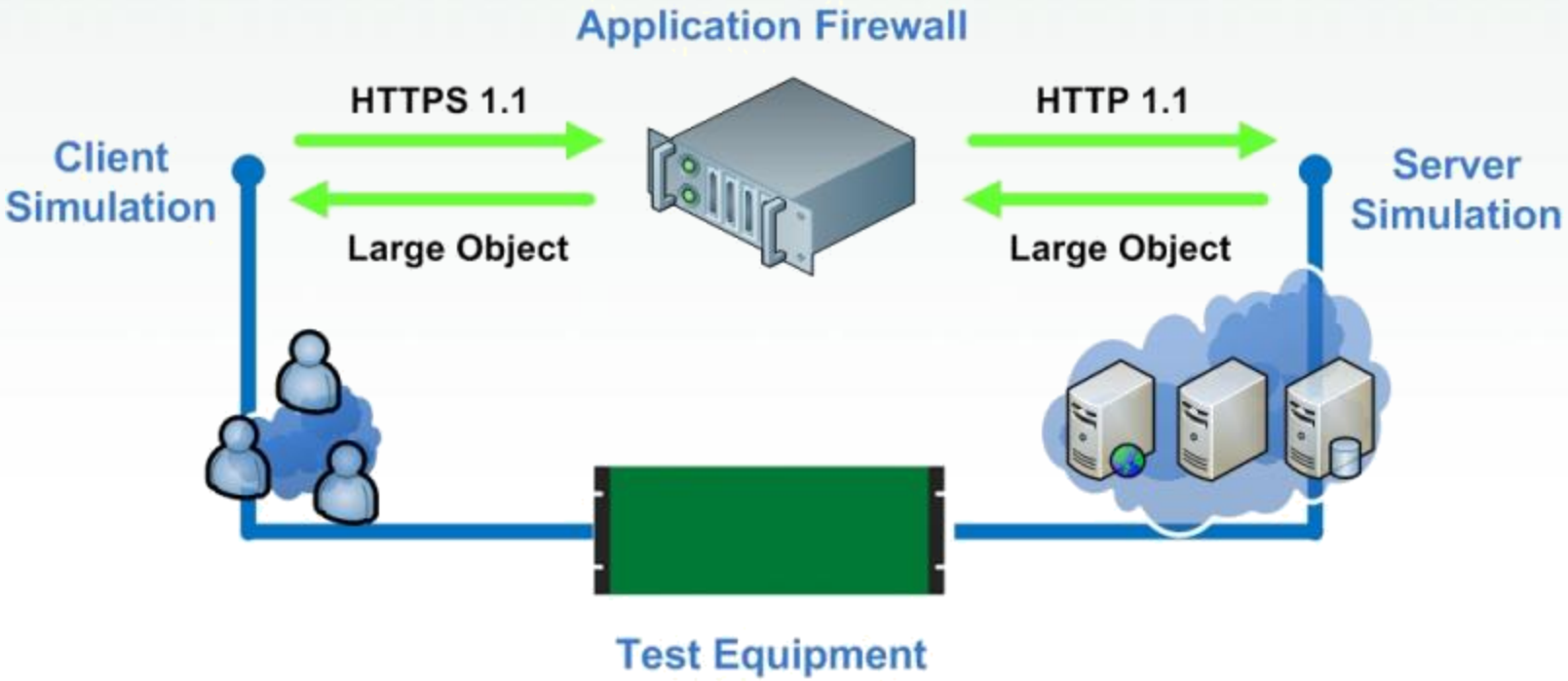
- Test Objective
  - Find the maximum HTTP bandwidth using several HTTP transactions over one TCP connection.
- Breaking Point
  - 100% of HTTP Transactions Successful
- Performance Measurement
  - Bandwidth
  - Maximum Concurrent TCP Connections
  - Average HTTP Transaction Response Time

Communication Via HTTP



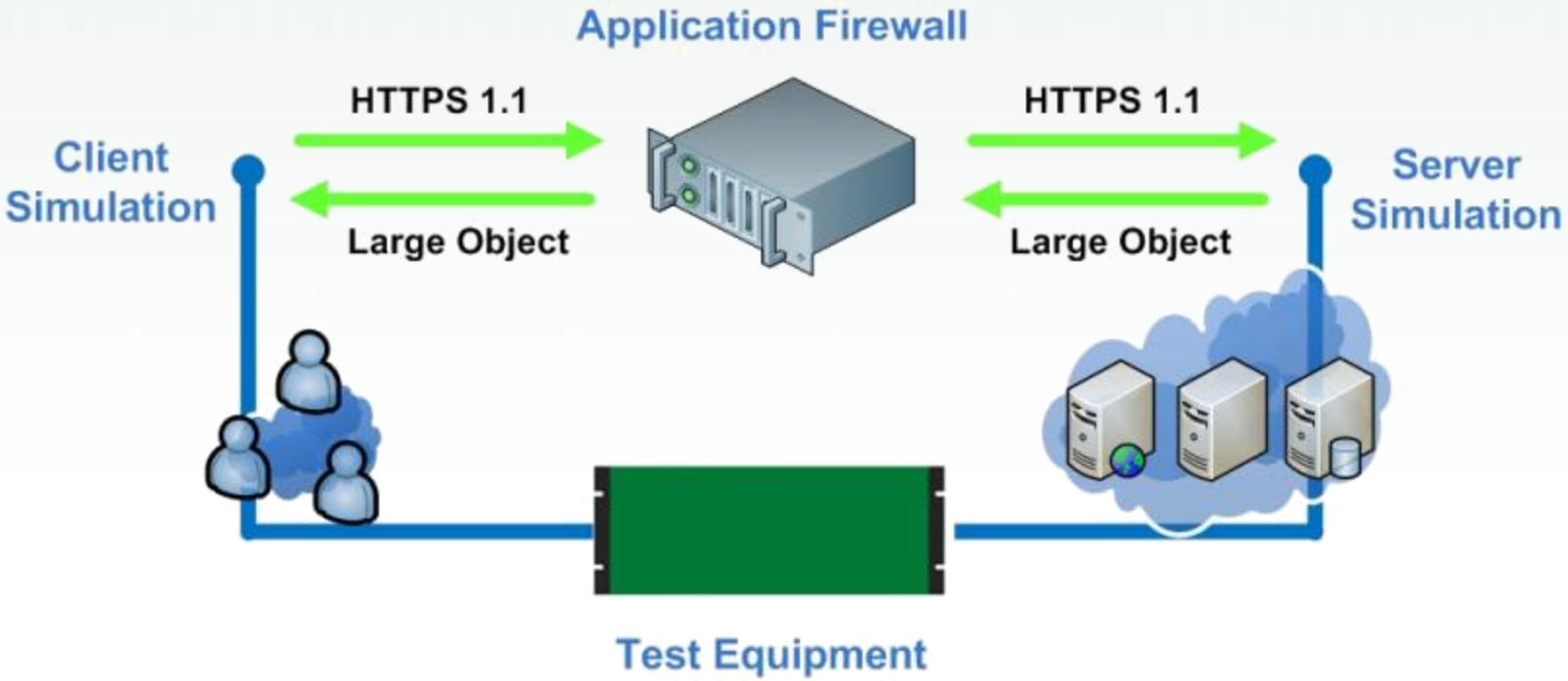
- Check performance using large object sizes like 1Mb

Communication Via HTTPS and HTTP



- Check performance using large object sizes like 1 Mb
- Check performance using different key sizes: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Communication Via HTTPS



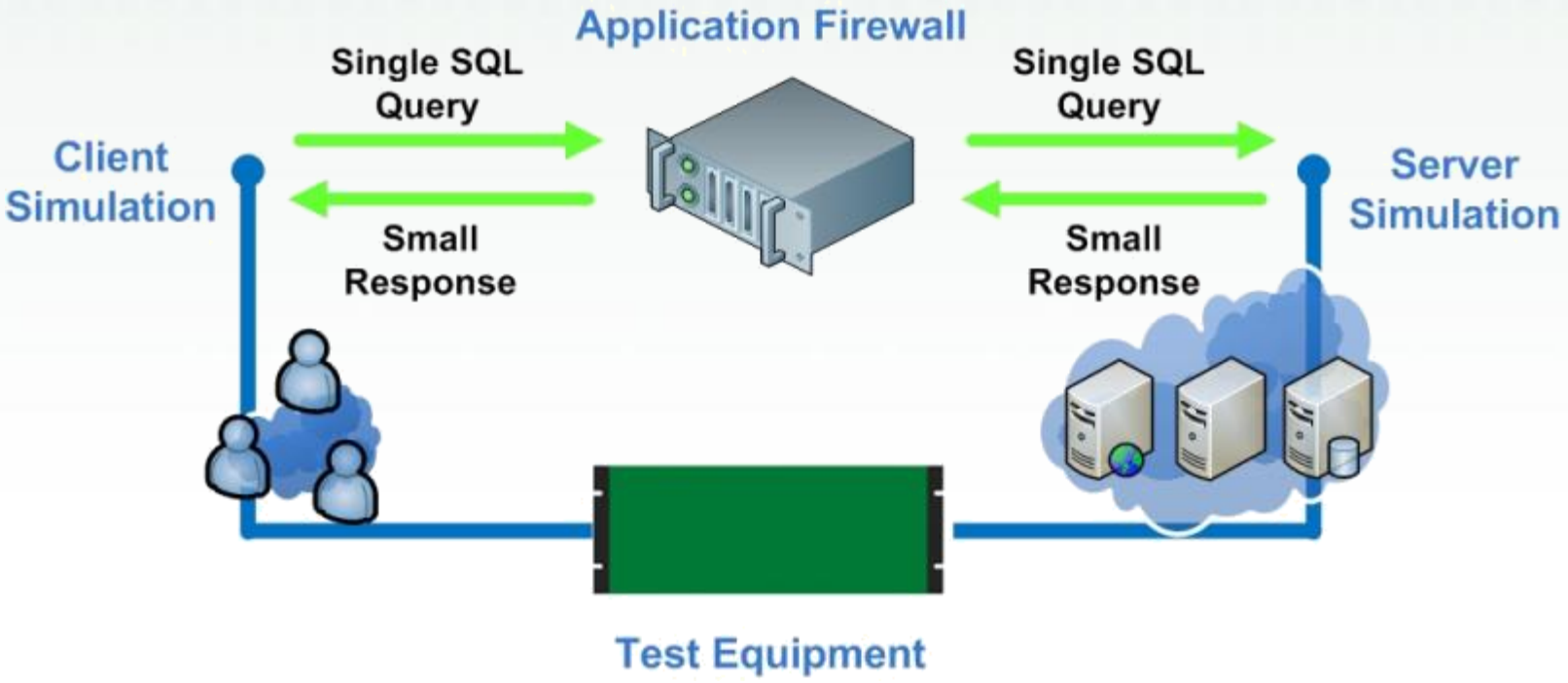
- Check performance using large object sizes like 1 Mb
- Check performance using different key sizes: 512, 1024 and 2048
- Check performance using different Cipher RC4-MD5, AES, …

Maximum Single SQL Queries per Second Supported by WAF

Maximum Single SQL Queries per Second

- Test Objective
  - Find the maximum SQL Queries per Second where one SQL query is sent over one TCP connection.
- Breaking Point
  - Low SQL Query Response Time
  - Low Number of Concurrent TCP Connections
  - 100% of SQL Queries Successful
- Performance Measurement
  - Maximum SQL Queries per Second
  - Average SQL Query Response Time
  - Maximum Concurrent TCP Connections
  - Bandwidth

Maximum Single SQL Queries per Second



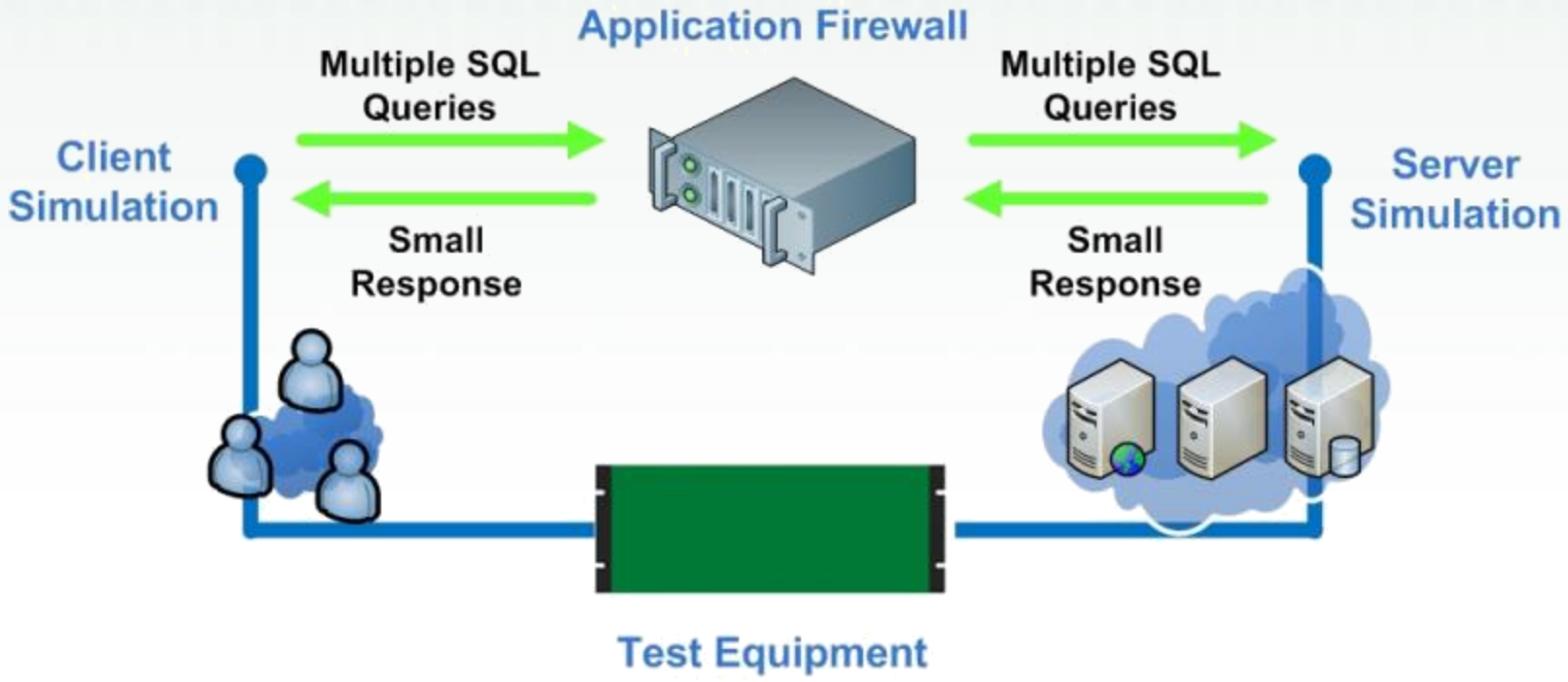
- Check performance using different query responses: 1024, 5120, 10240 and 51200

Maximum Multiple SQL Queries per Second Supported by WAF

Maximum Multiple SQL Queries per Second

- Test Objective
  - Find the maximum SQL Queries per Second where several SQL queries are sent over one TCP connection
- Breaking Point
  - Low SQL Query Response Time
  - Low Number of Concurrent TCP Connections
  - 100% of SQL Queries Successful
- Performance Measurement
  - Maximum SQL Queries per Second
  - Average SQL Query Response Time
  - Maximum Concurrent TCP Connections
  - Bandwidth

Maximum Multiple SQL Queries per Second



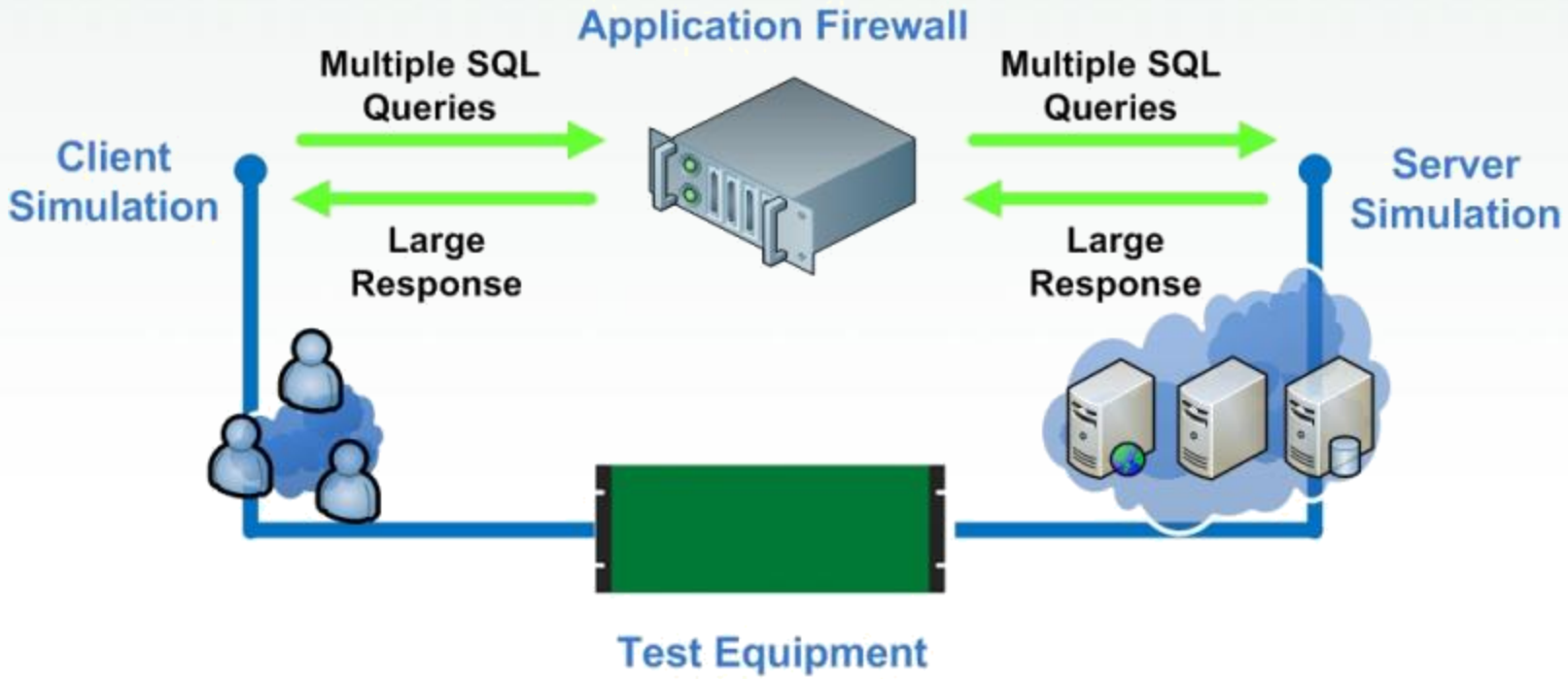
- Check performance using different query responses: 1024, 5120, 10240 and 51200

Maximum SQL Bandwidth Supported by WAF

Maximum SQL Bandwidth

- Test Objective
  - Find the maximum SQL bandwidth.
  - Several SQL queries are sent over one TCP connection
- Breaking Point
  - 100% of SQL Queries Successful
- Performance Measurement
  - Bandwidth
  - Maximum SQL Queries per Second
  - Maximum Concurrent TCP Connections

Maximum SQL Bandwidth



- Check performance using large response like 1Mb

WAF Performance
“Security Attacks”

Performance Security Testing

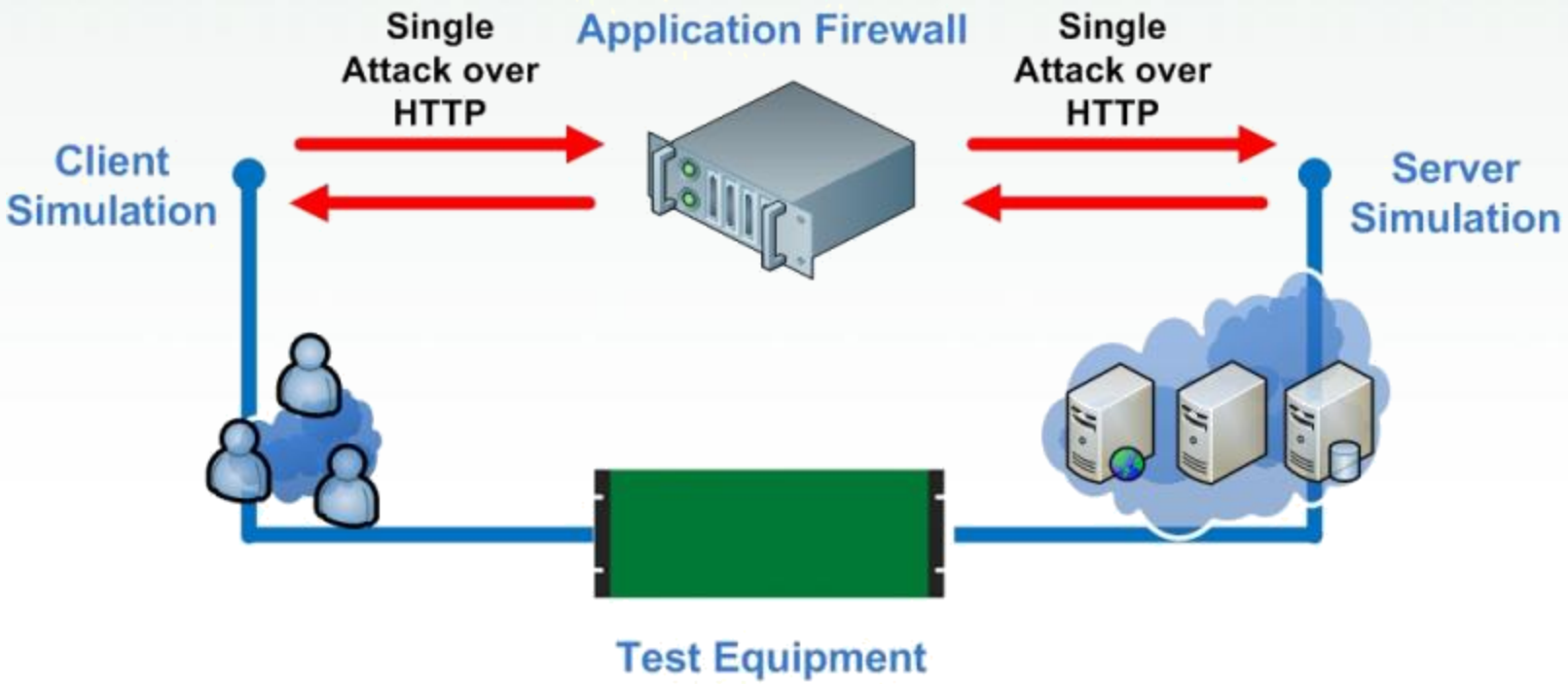
- Used attacks for performance testing under CVE-ID, OSVDB and BugTrag
- Ensure attack is detected before executing performance test
- Used attacks under the TOP 10 OWASP
  - A1 – Cross Site Scripting (XSS)
  - A2 – Injection Flaws
  - A3 – Malicious File Execution
  - A4 – Insecure Direct Object Reference
  - A5 – Cross Site Request Forgery (CSRF)
  - A6 – Information Leakage and Improper Error Handling
  - A7 – Broken Authentication and Session Management
  - A8 – Insecure Cryptographic Storage
  - A9 – Insecure Communications
  - A10 – Failure to Restrict URL Access

Maximum Single Type of HTTP Attacks per Second Detected by WAF

Maximum Single HTTP Attacks per Second

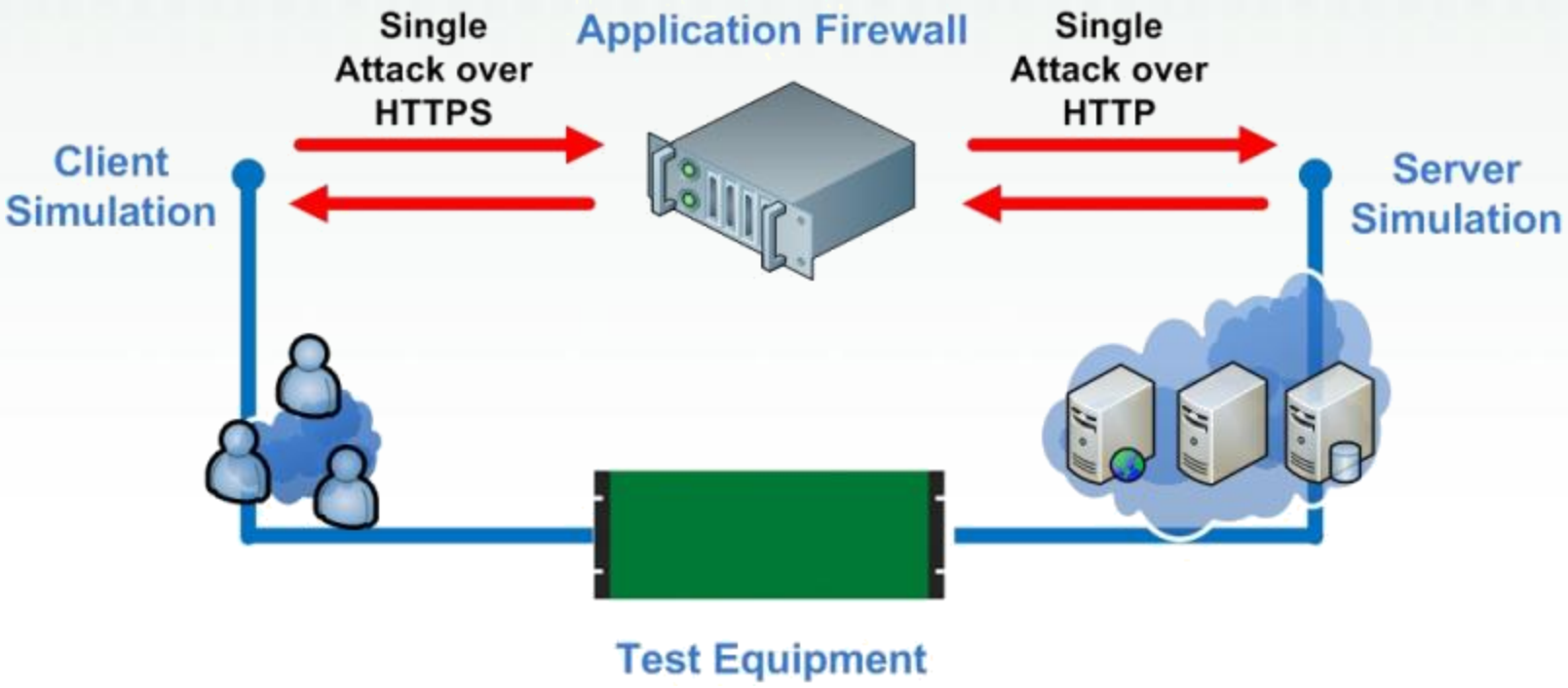
- Test Objective
  - Find the Maximum Attacks per Second detected.
  - The same attack is used during entire test.
- Breaking Point
  - Number of Attacks per Second sent doesn't match with number of Attacks detected
- Performance Measurement
  - Maximum Attacks per Second detected

Communication Via HTTP



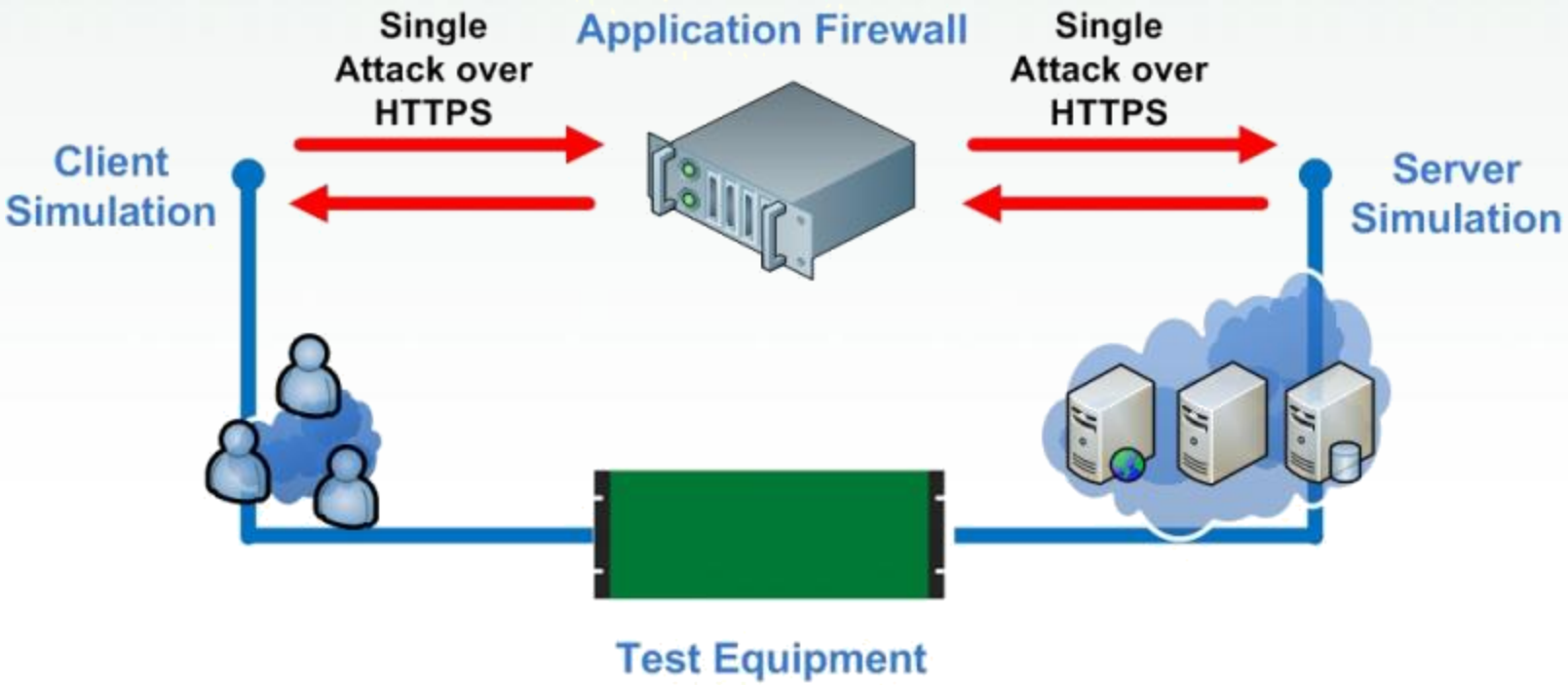
- Check number of attacks detected versus the number of attacks of attacks sent

Communication Via HTTPS



- Check number of attacks detected versus the number of attacks of attacks sent

Communication Via HTTPS



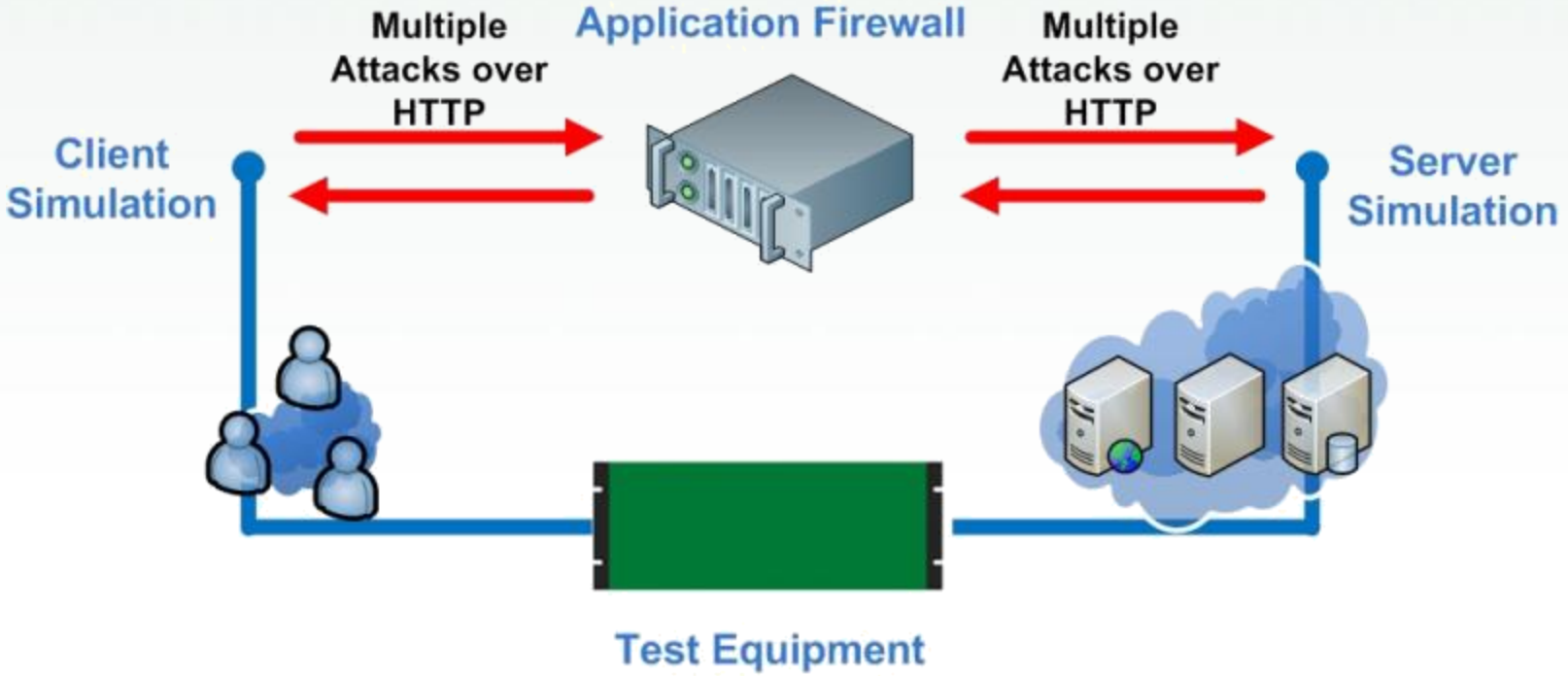
- Check number of attacks detected versus the number of attacks of attacks sent

Maximum Multiple Types of HTTP Attacks per second Detected by WAF

Maximum HTTP Attack per Second

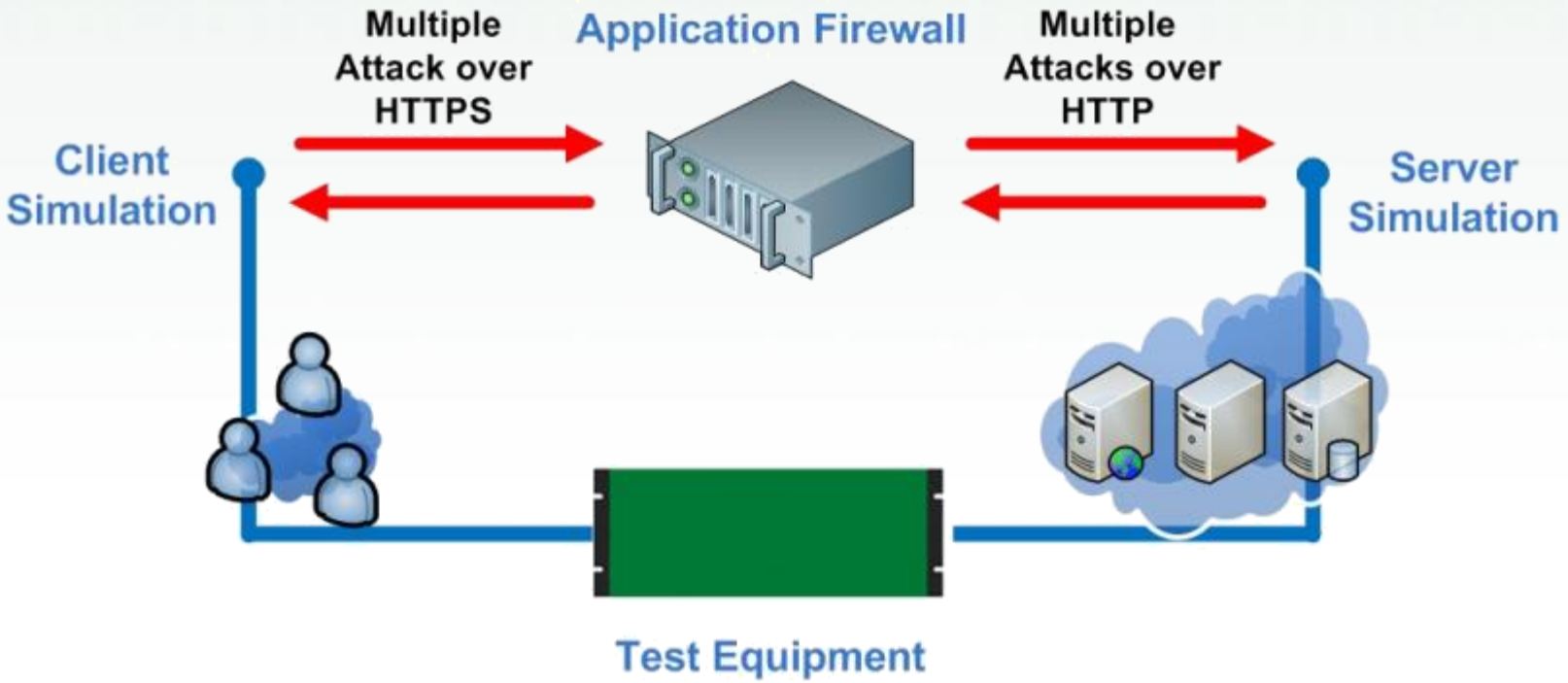
- Test Objective
  - Find the Maximum Attacks per Second detected.
  - Mix of different types of attacks (TOP 10 OWASP) are used during the entire test.
- Breaking Point
  - Number of Attacks per Second Send doesn't match with number of Attacks Detected
- Performance Measurement
  - Maximum Attacks per Second detected

Communication Via HTTP



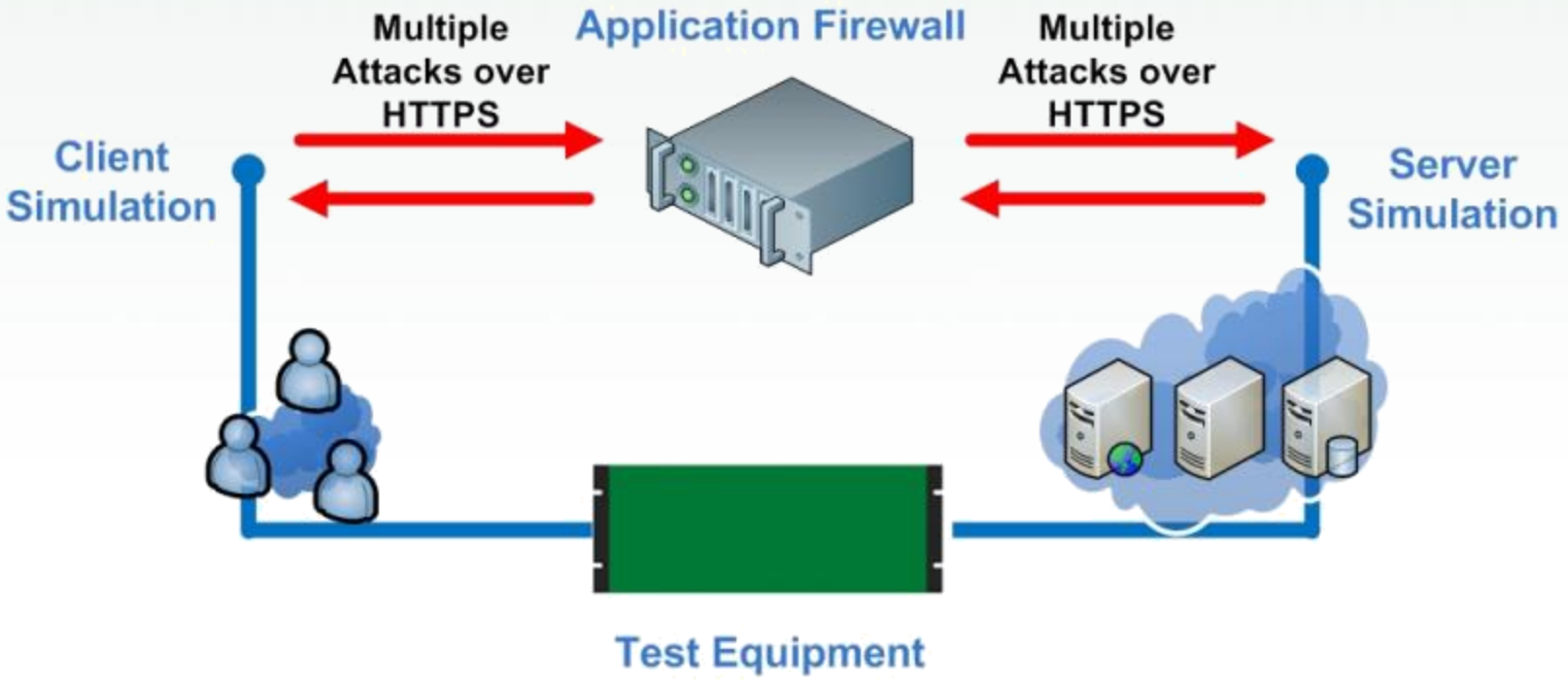
- Check number of attacks detected versus the number of attacks of attacks sent

Communication Via HTTPS and HTTP



- Check number of attacks detected versus the number of attacks of attacks sent

Communication Via HTTPS



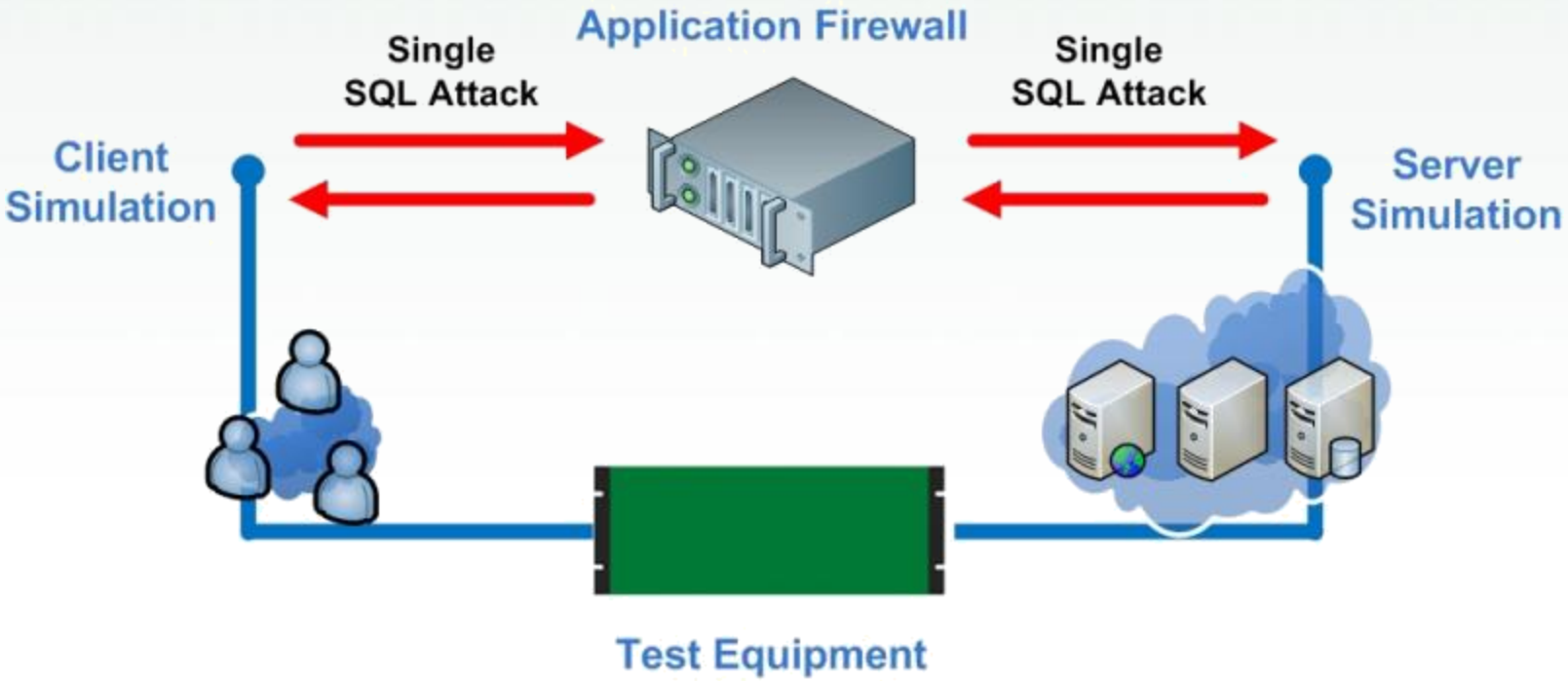
- Check number of attacks detected versus the number of attacks of attacks sent

Maximum Single
SQL Attacks per second
Detected by WAF

Maximum SQL Attacks per Second

- Test Objective
  - Find the Maximum Attacks per Second detected.
  - The same SQL attacks are used during the entire test.
- Breaking Point
  - Number of Attacks per Second sent doesn't match with number of Attacks Detected
- Performance Measurement
  - Maximum Attacks per Second detected

Maximum SQL Attacks per Second



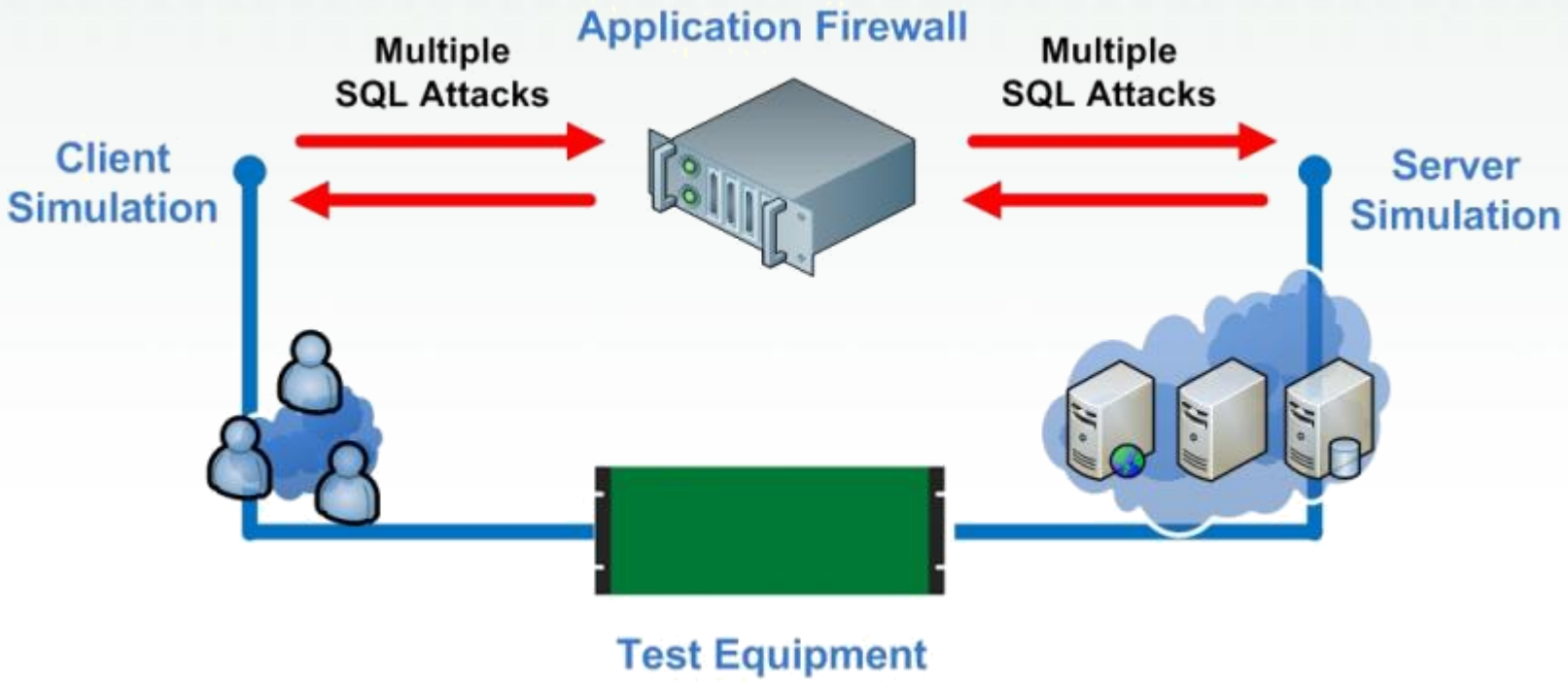
- Check number of attacks detected versus the number of attacks of attacks sent

Maximum Multiple Type SQL Attacks per second Detected by WAF

Maximum SQL Attacks per Second

- Test Objective
  - Find the Maximum Attacks per Second detected.
  - Mix of different types attacks are used during the entire test.
- Breaking Point
  - Number of Attacks per Second Sent doesn't match with number of Attacks Detected
- Performance Measurement
  - Maximum Attacks per Second Detected

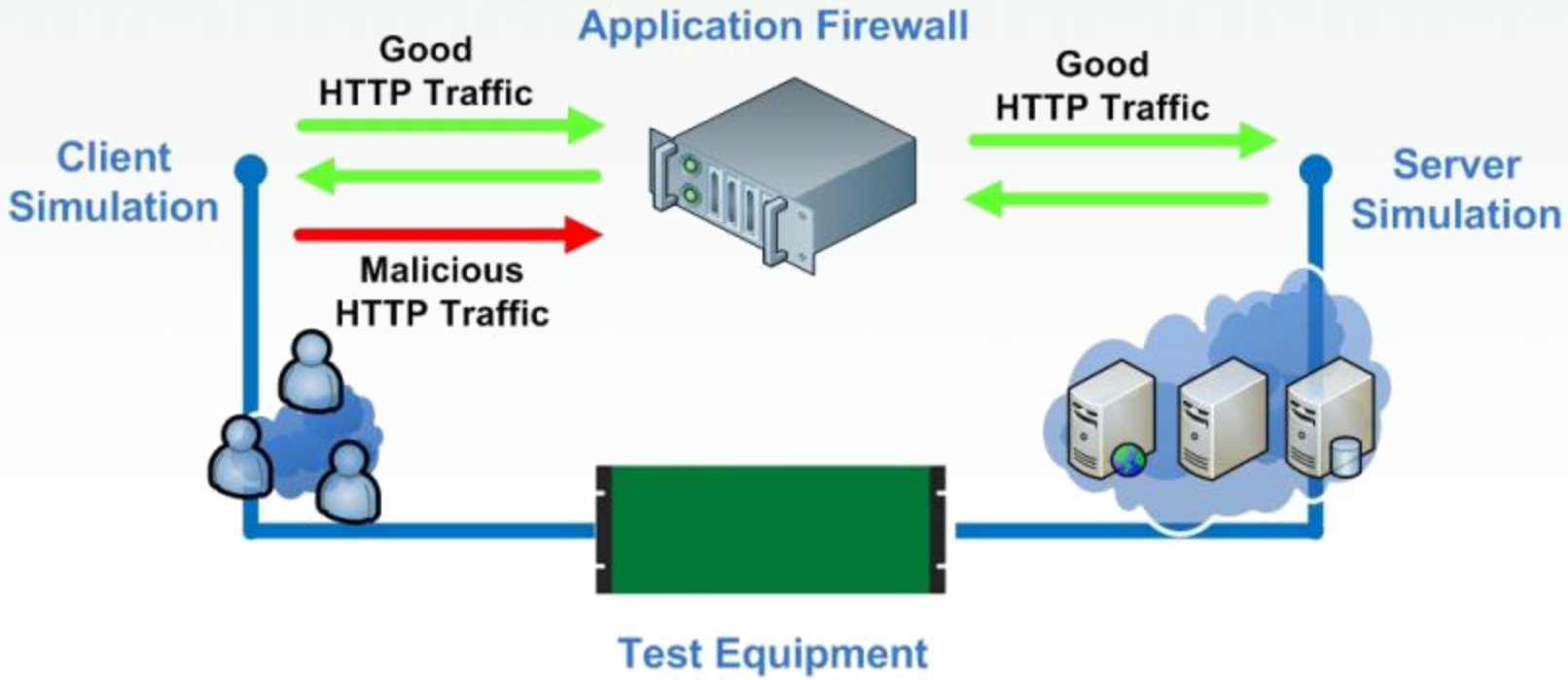
Maximum SQL Attacks per Second



- Check number of attacks detected versus the number of attacks of attacks sent

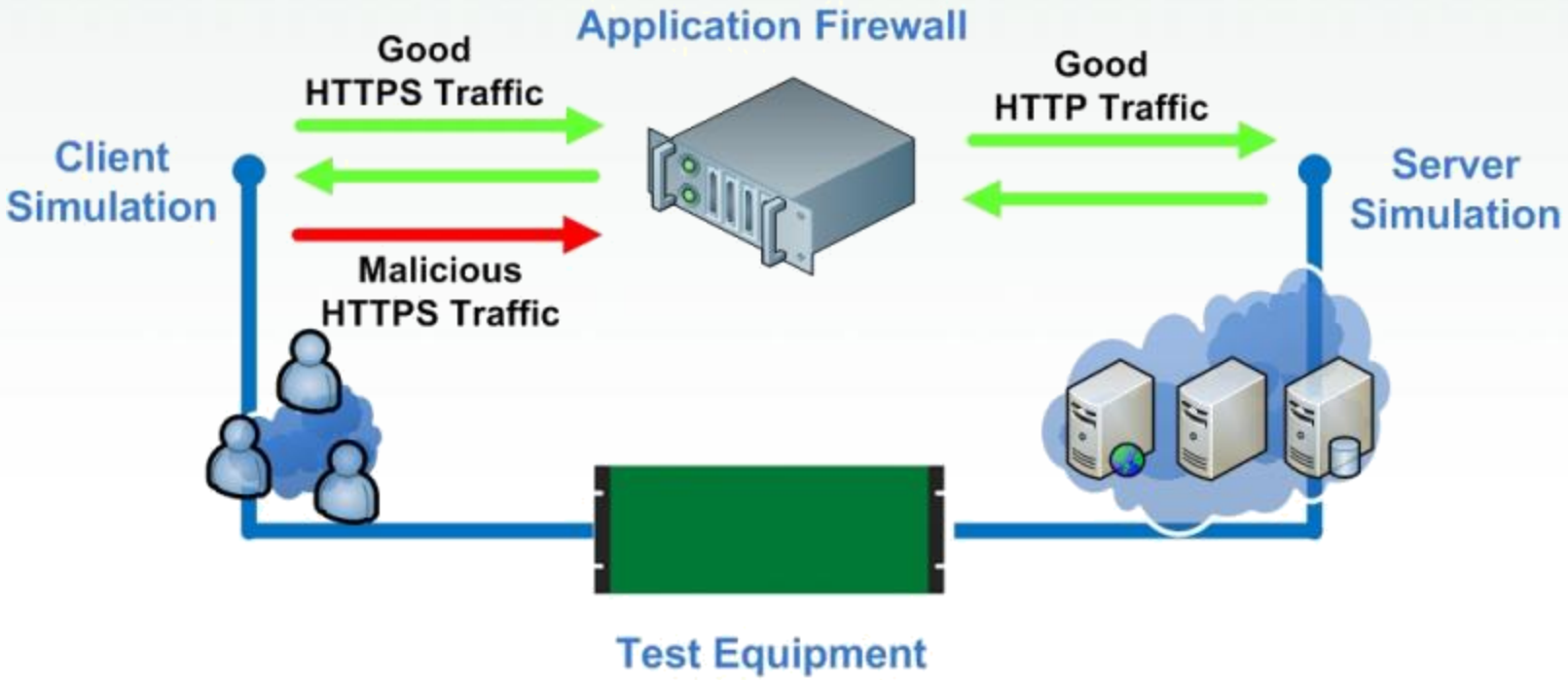
WAF Performance
Good Traffic
and Security Attacks

Communication Via HTTP



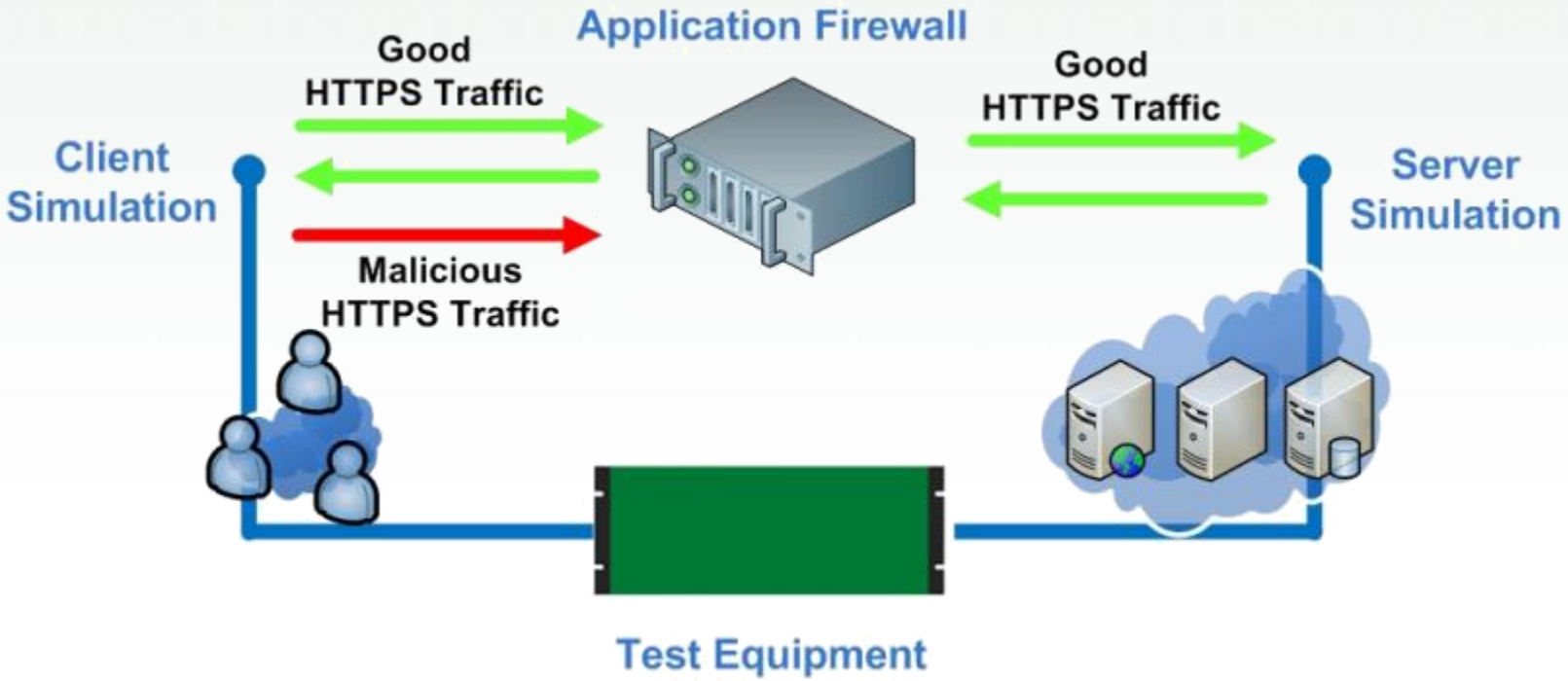
- Check performance in terms of Transactions per Second
- Check number of attacks detected versus the number of attacks sent

Communication Via HTTPS and HTTP



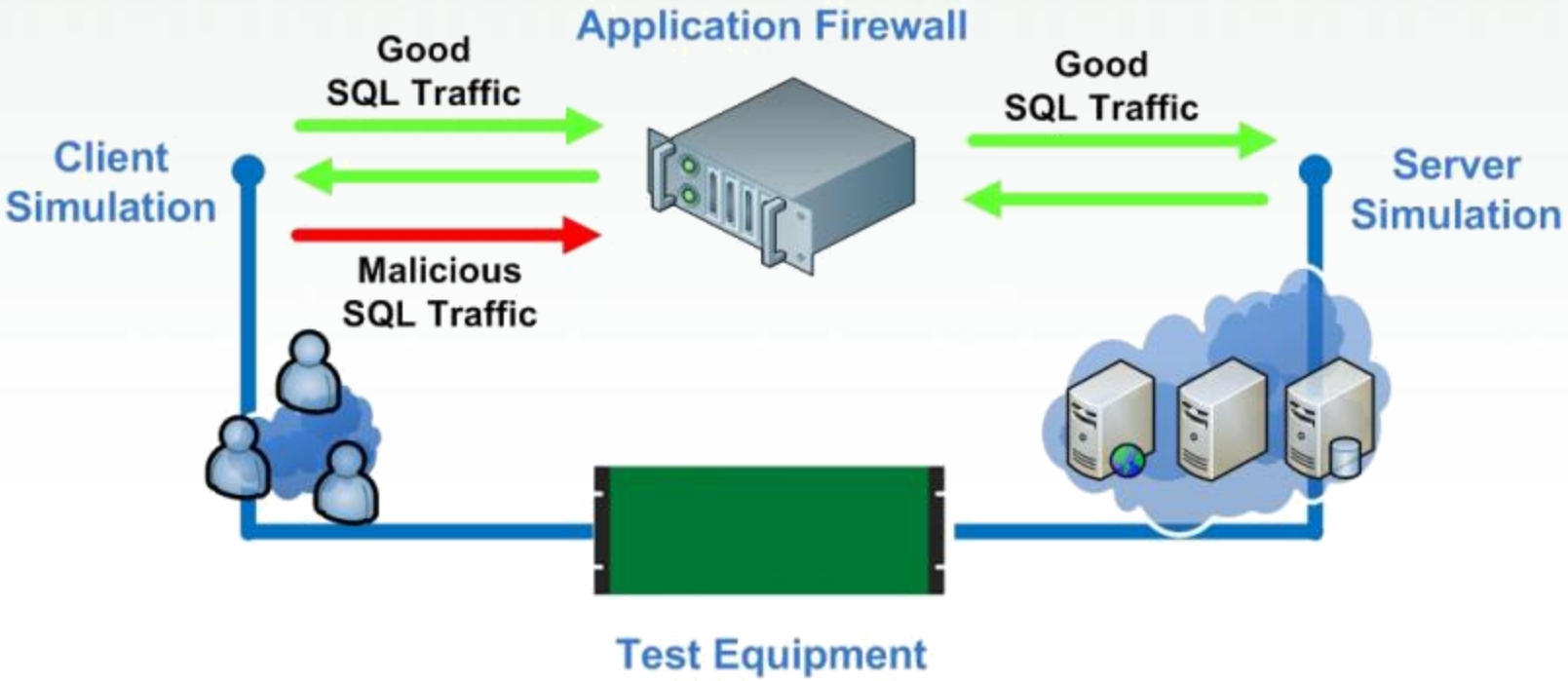
- Check performance in terms of Transactions per Second
- Check number of attacks detected versus the number of attacks of attacks sent

Communication Via HTTPS



- Check performance in terms of Transactions per Second
- Check number of attacks detected versus the number of attacks of attacks sent

Maximum Single SQL Queries per Second



- Check performance in terms of SQL Queries per Second
- Check number of attacks detected versus the number of attacks of attacks sent

Maximum
WAF Performance
“Real-World Test Scenario”

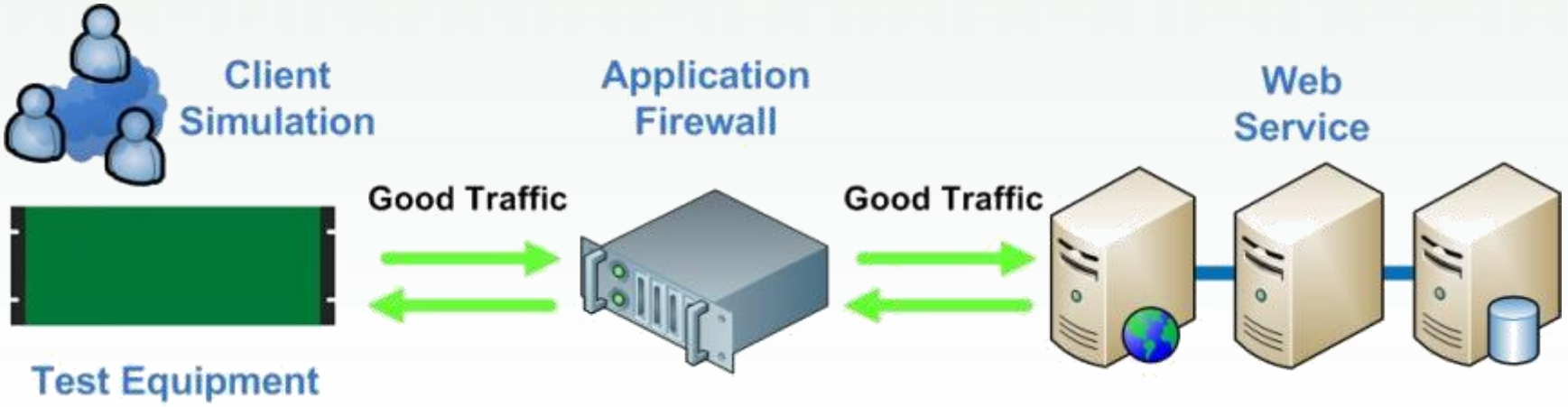
Real-World Test Scenario - WAF Test Methodology

- Test is performed on WAF Vendor selected
- Web Service Performance without WAF
  - Maximum New Users per Second
  - Maximum Concurrent Users
  - Maximum Bandwidth
- Web Service Performance with WAF
  - Maximum New Users per Second
  - Maximum Concurrent Users
  - Maximum Bandwidth
- Web Service Performance and Security with WAF
  - Mix Good Traffic and Security Attacks

Web Service Performance Without WAF

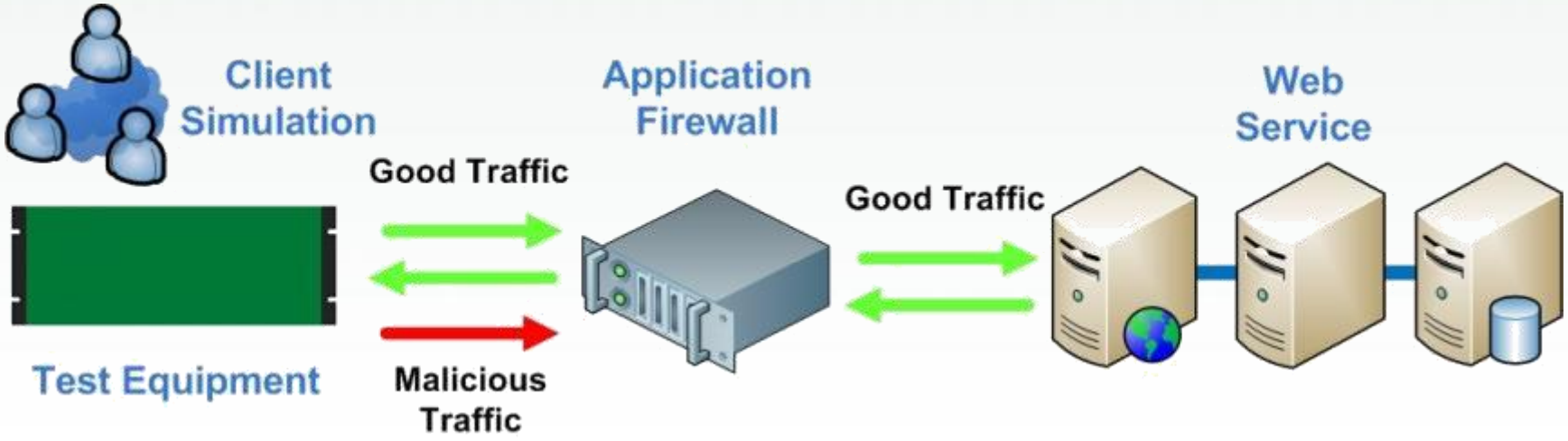
- Check Maximum New Users per Second of Web Service
- Check Maximum Concurrent Users of Web Service
- Check Maximum Bandwidth of Web Service

Web Service Performance With WAF



- Check Maximum New Users per Second of Web Service
- Check Maximum Concurrent Users of Web Service
- Check Maximum Bandwidth of Web Service

Web Service Performance and Security With WAF



- Check Maximum New Users per Second of Web Service
- Check Maximum Concurrent Users of Web Service
- Check Maximum Bandwidth of Web Service
- Check All Attacks Sent are Detected by WAF

Key Benefits of Web Application Firewall Testing

Better Visibility of WAF Performance

- Know the real performance of your WAF – Performance Matrix
  - Maximum HTTP Transactions per Second
  - Maximum HTTPS Transactions per Second
  - Maximum SQL Queries per Second
  - Maximum Concurrent TCP Connections
  - Maximum Concurrent SSL Sessions
  - Maximum HTTP Bandwidth
  - Maximum HTTPS Bandwidth
  - Maximum SQL Bandwidth
- You know the real capacity of your WAF – Performance Matrix
  - Maximum New Users per Second
  - Maximum Concurrent Users

Better Visibility of WAF Performance

- Choose the best WAF for your needs
- Deploy your WAF in the right configuration for optimal performance
- Be more proactive because you know how your WAF will behave under load and attacks

Contact Information

For more Information for Israel contact WebHouse:

Alon Refaeli: refaeli@WebHousePlus.com +972525873337

Amir Pled: amir@WebHousePlus.com +972542489595

For more information outside of Israel contact BreakingPoint Systems:

Gregory Fresnais: gfresnais@bpointsys.com +33672510922

Thank You

www.breakingpoint.com