
HAFS
Distributeur à valeur ajoutée
VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES
EXPERTISE
Des solutions adaptées à chaque environnement
CONFIANCE
Un partenaire fiable à vos côtés
PERFORMANCE
Des infrastructures sécurisées et évolutives
SUPPORT
Un accompagnement technique de qualité
HAFS
Distributeur à valeur ajoutée
Des solutions IT innovantes pour un monde connecté et sécurisé
WIRELESS RADIO
Connectivité sans fil haute performance
RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés
VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives
CYBERSECURITY
Protéger vos données et vos systèmes
VIDÉO PROTECTION
Solutions de vidéosurveillance intellligentes
HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité
SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

Hillstone Web Application Firewall (WAF)

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

Agenda

- Business Problem
- Introduction of Hillstone WAF
- Model Selection & Ordering Information
- Deployment Modes & Use Cases
- Case Studies

Business Problem

Key Problems:
More Threats From Web Application

Invasion Threat

High-risk applications cause more threat intrusion

Information Leakage

Use of unauthorized applications can easily lead to data leakage

Rising Cost

Bandwidth abuse leads to rising operating costs

Productivity Decline

Uncontrolled application usage reduces employee productivity

DDoS attack, CC attack, SQL injection…

Nowadays, more than 75% of threats occur in web application

What Can WAF Provide?

Web Application Firewalls are the ***fastest and most cost-effective*** way to address application vulnerabilities in production

APP Protection

- Coverage for OWASP Top 10:
  - XSS
  - Injection
  - Bot Mitigation
  - Malware
  - …
- Protection over other unknown threats

Network Protection

- Protection of DoS attacks
- Protection of Flood attack
- Protection of IP/port scanning and spoofing
- Protection of TCP anomalies
- Protection of Malicious IP

API Protection

- Brute Force mitigation
- L7 DoS
- API schema validation
- Security policy updates

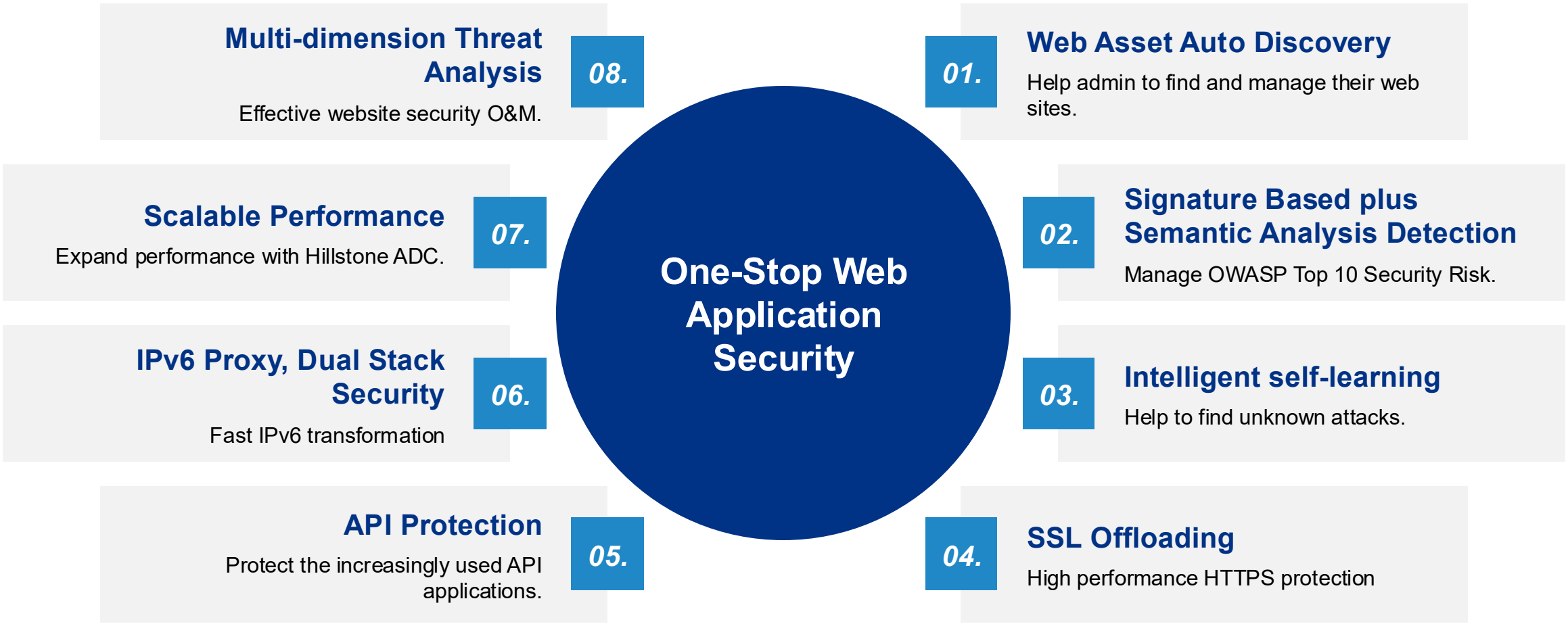
When Do You Use WAF In A Security Solution

Product positioning in a security solution: NGFW vs IPS vs WAF

	FW	IPS	WAF
			
Analogy	The Gate	The Guard	The Bodyguard
Technique	Policy	Signatures	Proxy
Service	All traffic	All traffic	HTTP/HTTPS
Size of the purchase	8	4	1

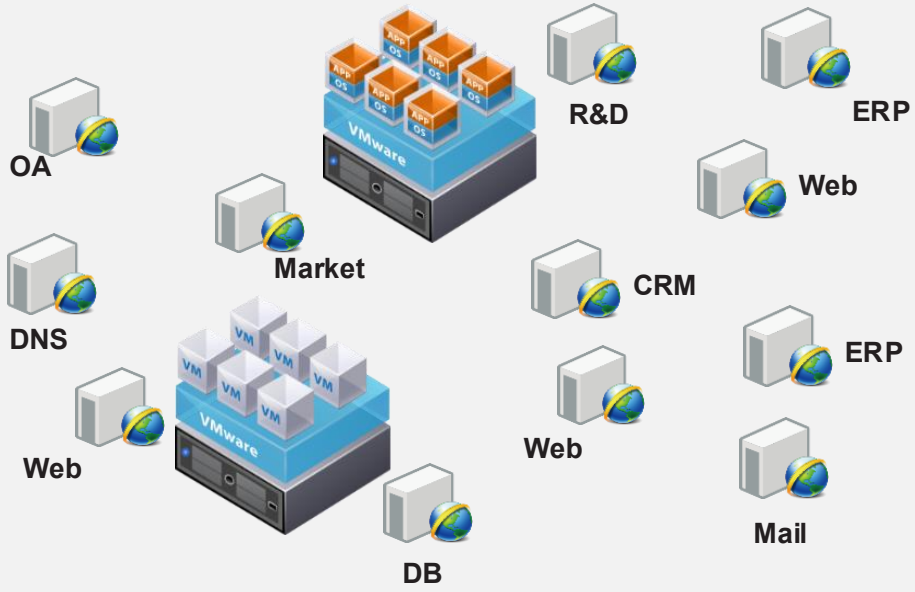
Introduction of Hillstone WAF

Hillstone Web Application Firewall Overview



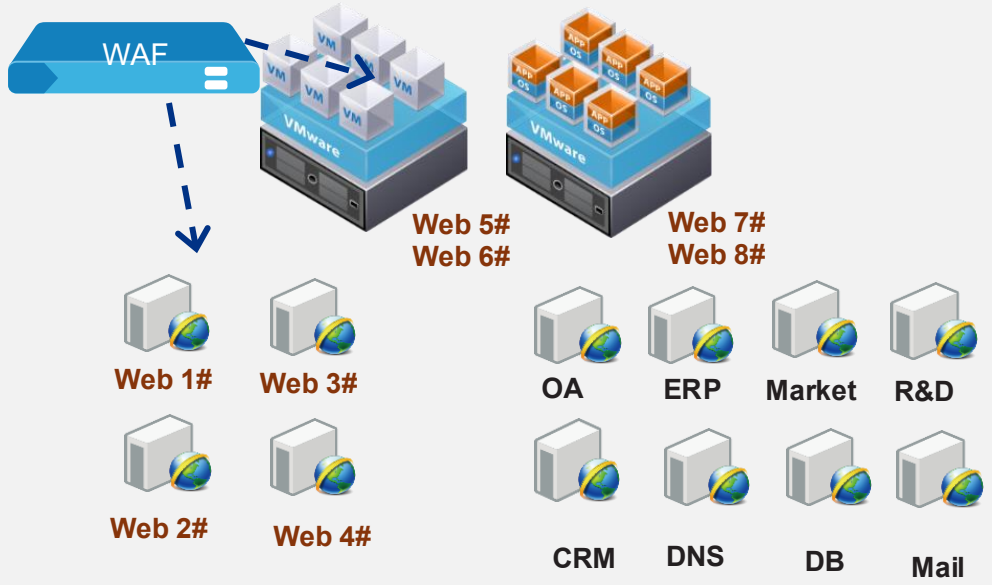
Simplify Operations through Automatic Website Asset Discovery

Before: 24 hour or Days



- How to sort out hundreds of Web services that need protection?
- Fill the form, IP/port/domain name statistics, etc.

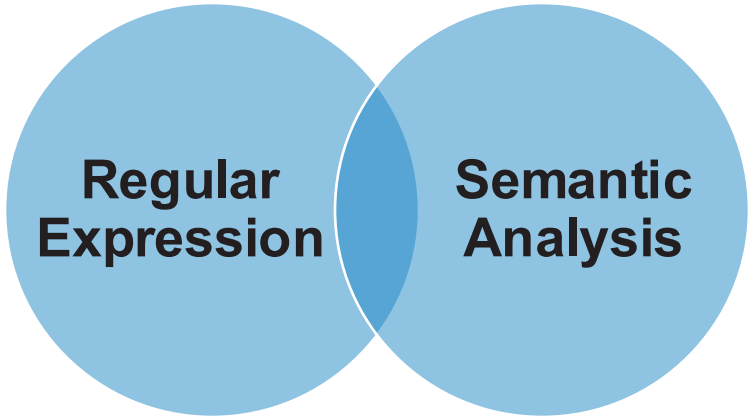
Now: 20 min



- Automatically detect web traffic in the network through asset self-discovery; discover and define web services and assets.

Complete OWASP Risk Mitigation and Resolution

OWASP
TOP10 Security Risks (2017)



Hillstone WAF using dual detection engines to find attacks like SQL injection and XSS with higher precision than regular expression WAF, and thus help customer to mitigate OWASP Top10 web application risks.

*The Open Web Application Security Project (OWASP) is a non-profit foundation dedicated to improving the security of software. OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical web application security risks.

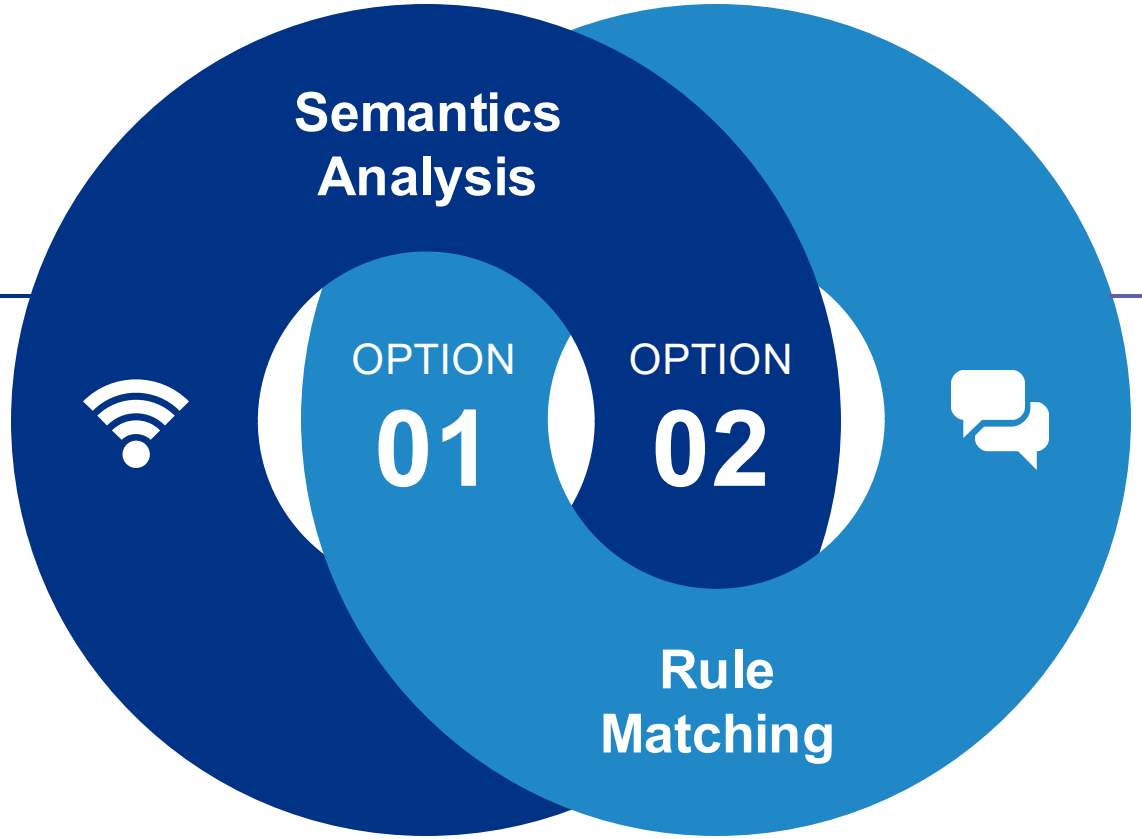
- A1 Injection
- A2 Broken Authentication
- A3 Sensitive Data Exposure
- A4 XML External Entities (XXE)
- A5 Broken Access Control
- A6 Security Misconfigurations
- A7 Cross Site Scripting (XSS)
- A8 Insecure Deserialization
- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging and Monitoring

Dual Detection Engine - Semantics Analysis + Rule Matching

Dual Detection Engine

Semantic Analysis

- XSS Semantics Detection
- SQL Injection Detection
- Recursive Decoding



30% decrease in false positive

Rule Matching

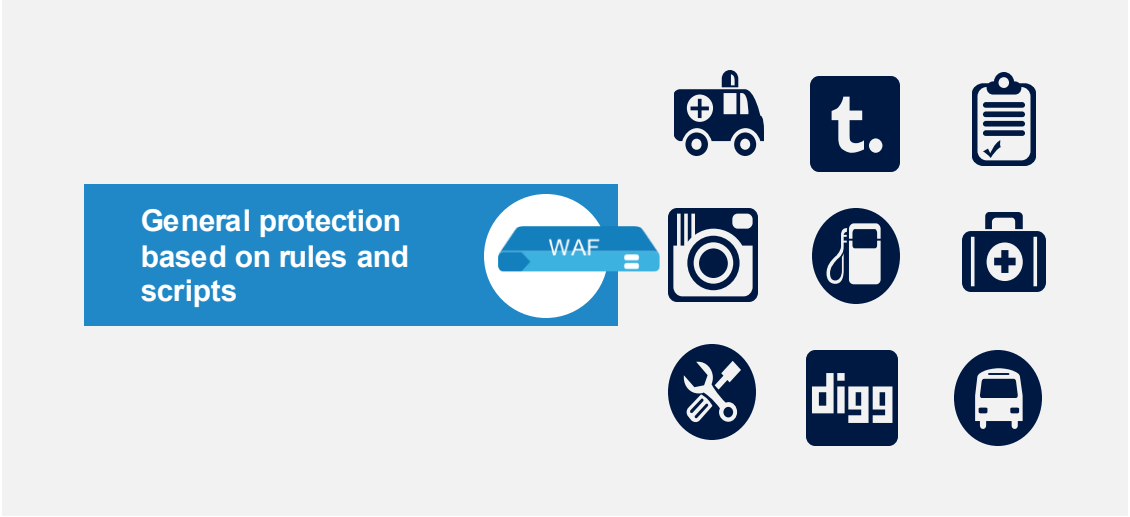
- Regular Expression
- False positive Remediation
- Recursive Decoding

Comprehensive Defense Against Injection Attack

- In addition to the most common SQL injection, Hillstone WAF can detect and defend against various other injection attacks.
- 10+ injection attacks, 200+ injection detection rules.

- SQL Injection
- LDAP Injection
- PHP Code Injection
- XML Injection
- Email Injection
- Remote File Inclusion (RFI)
- Server-Side Includes Injection(SSI)
- Local File Inclusion (LFI)
- XPath Injection
- JavaScript Injection
- Command Injection
- Other Injections…

Machine Learning Based Customized Protection



Learn	Revision	Protection
• Parameter length, type • Cookie • HTTP operation method • Client IP distribution	• Administrator optimization • Learning result correction	• Dynamic URL tree • Generate an exclusive protection strategy • Detect the unknown attacks

Anti-Defacement For Dynamic & Static Contents

Kernel Driver Level Protection

APPLICATION

I/O MANAGMENT

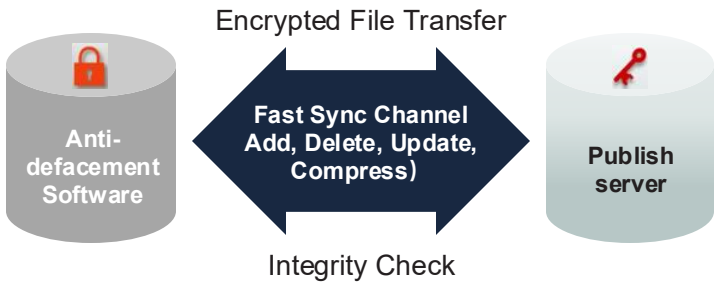
DRIVER FILTERING

FILE SYSTEM

FILE STORAGE

Web Server File Access

Safe & Reliable Increment Synchronization



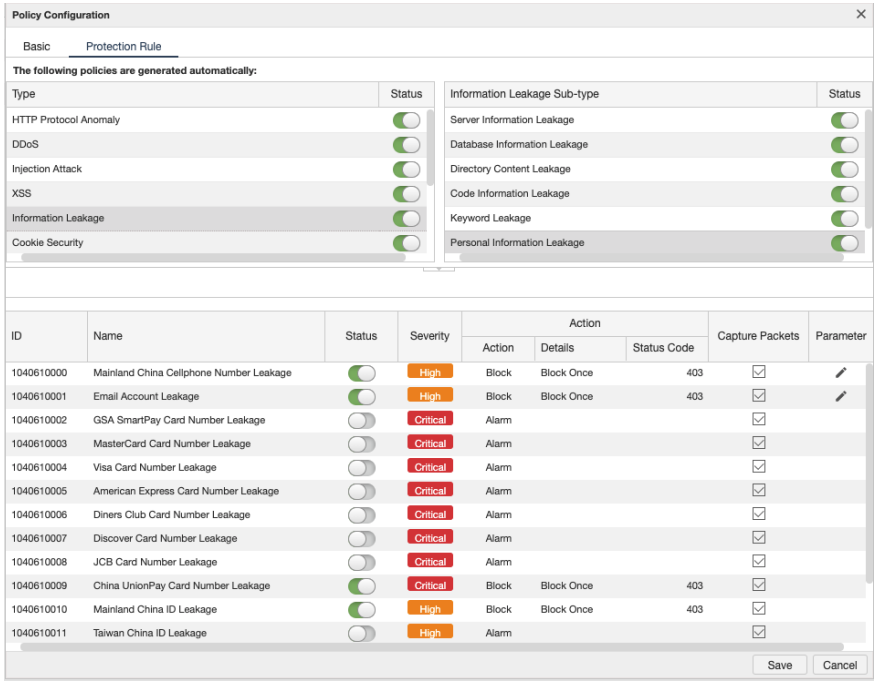
Static& Dynamic Contents

Sensitive Information Protection (Web)

- Hide Personal information & sensitive words (with *)
- No impact to normal business

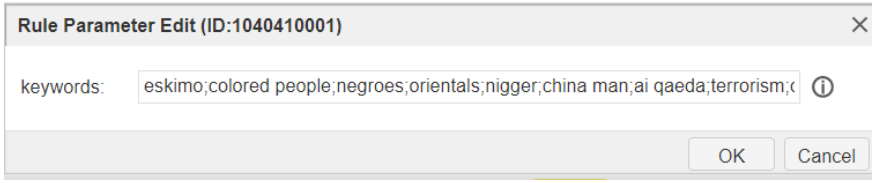
Personal Information

Cell phone, email, ID card, bank card number leakage



Sensitive Words

Sensitive political tendency, violent tendency, unhealthy color

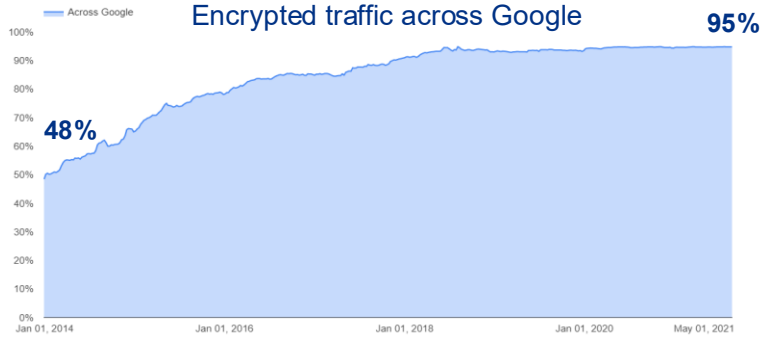


Before desensitization

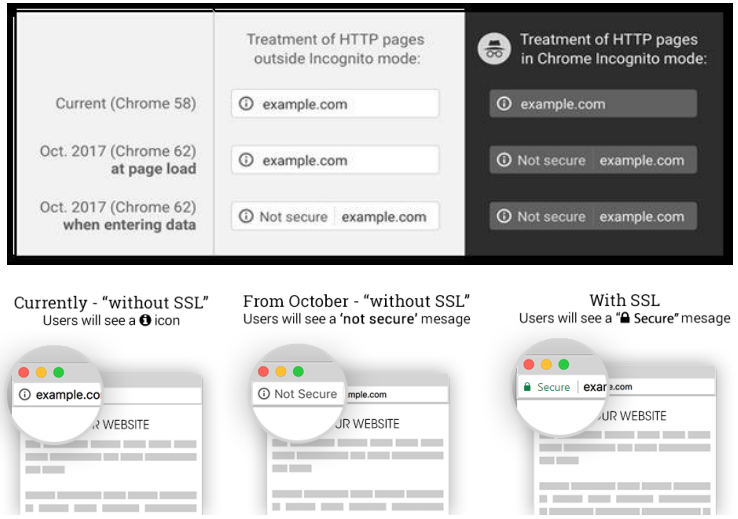
After desensitization

Detect Attacks in Encrypted Traffic

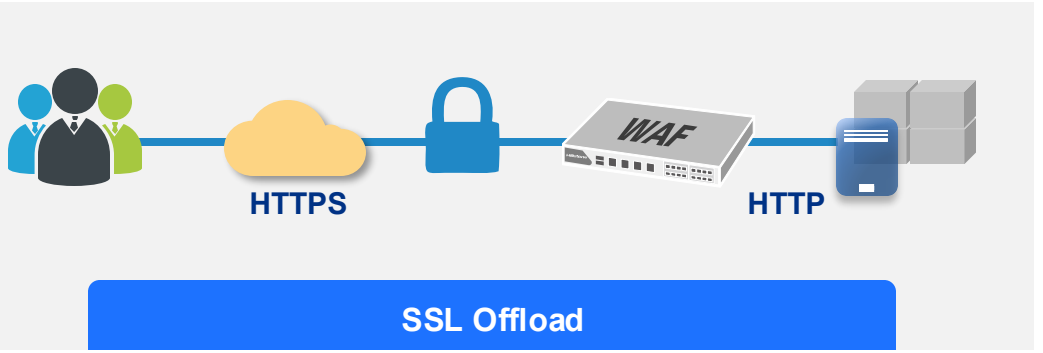
95% of the traffic across Google has been encrypted.

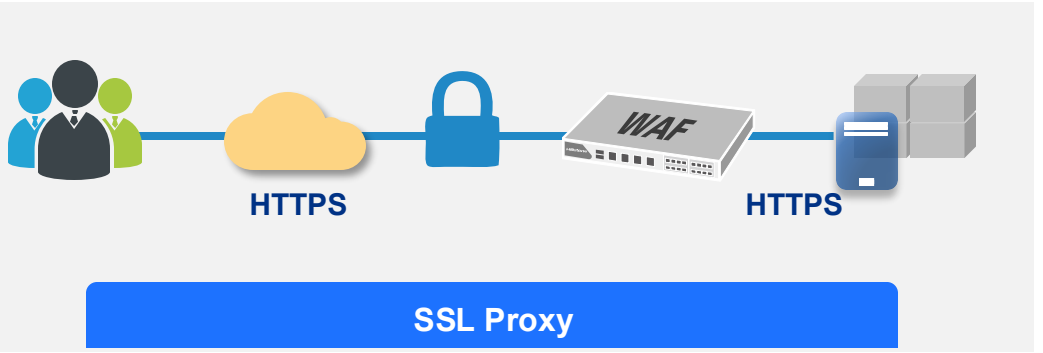


Google marks http web as unsafe.

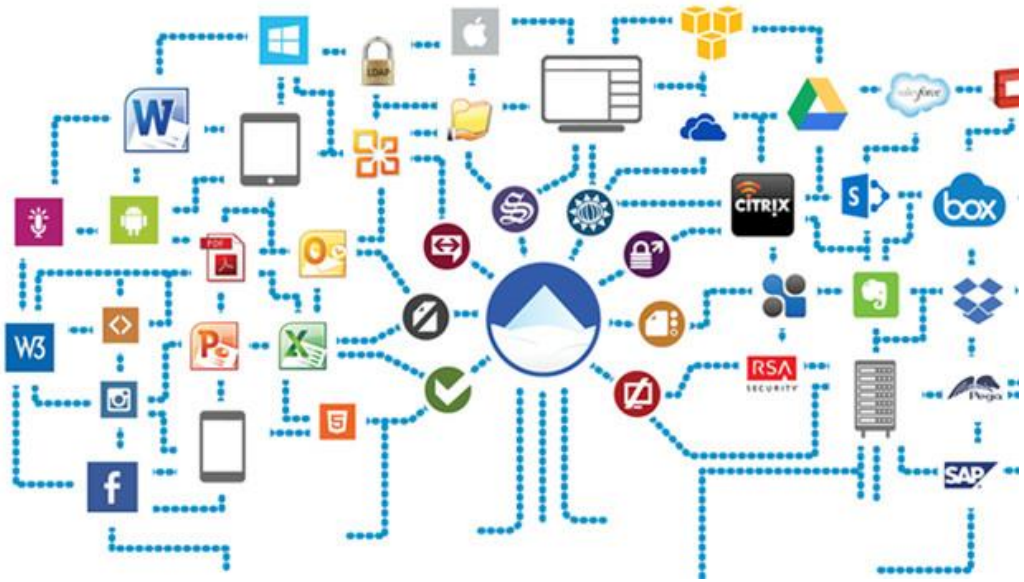


Seamlessly upgrade the website to HTTPS and provide comprehensive protection using Hillstone WAF





API Protections



OWASP

OWASP API Security Top 10 2019

The Ten Most Critical API Security Risks

API Scenarios

- API are software intermediary that allows two applications to talk to each other, and now widely used in modern apps.
- Online shopping, booking, weather, map, stock…

Risks

- Excessive data exposures via API
- Injection and XSS attacks among API calls
- Refer to OWASP Top 10 API Security

Hillstone Provides

- Attacks detection in API
- Schema Validation according to OpenAPI file

API Protection - Compliance

Typical Scenario:
- Online Shopping
- Financial Transactions
- Hospital Registration
- Smart City
- Others

Risk
- API exposes a lot of information to the public and raises more potential risks

Solution:
- **API Protection - Compliance**

Schema Validation

User Definition

API Specification

Import OpenAPI File
- json
- yaml
- yml

Customized Rules

Customized Configuration
- HTTP host
- URI

IPv6 Protection and Fast IPv6 Transformation

01

Support IPv4/IPv6 dual-stack deployment

02

Support IPv6 access proxy

03

Provide IPv6 services without upgrading IPv4 application server, and IPv4 access is not affected.

Value:

Support IPv6 transformation

Scenario:

Limited budget;
IPv6 transformation of websites with external links

Layer 3 Access Control

FW Policy

- Support access control based on Src & Dst Zone/IP/Port, Service, Schedule, etc.

FW Policy Optimization

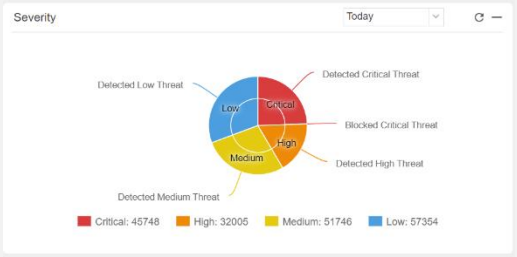
- FW policy hit analysis
- FW policy redundancy detection
- FW policy assistant: automate policy creation based on traffic learning

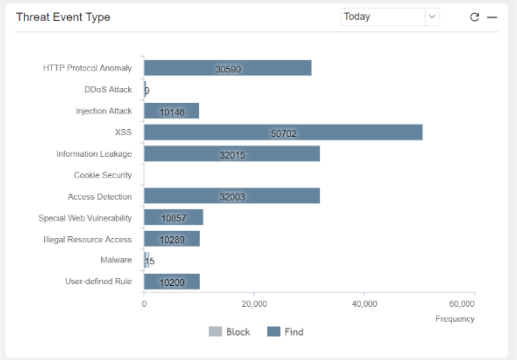
Session Logging

- Comprehensive session data logging for auditing and diagnostics

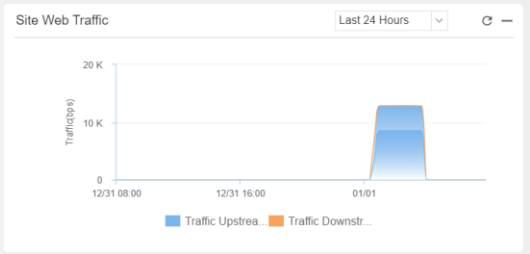
Multi-dimensional Visibility for Efficient O&M

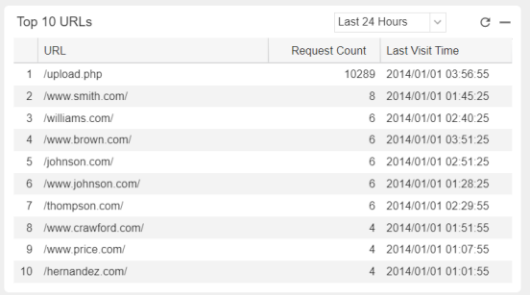
Threat Analysis





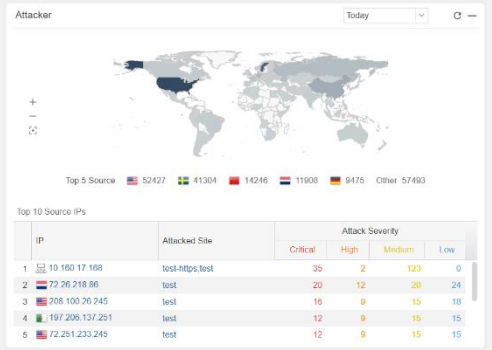
Traffic Analysis

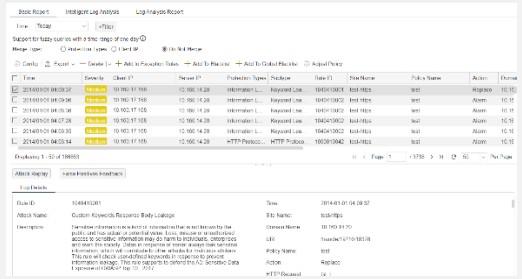




	URL	Request Count	Last Visit Time
1	/upload.php	10289	2014/01/01 03:56:55
2	/www.smith.com/	8	2014/01/01 01:45:25
3	/williams.com/	6	2014/01/01 02:40:25
4	/www.brown.com/	6	2014/01/01 03:51:25
5	/johnson.com/	6	2014/01/01 02:51:25
6	/www.johnson.com/	6	2014/01/01 01:28:25
7	/thompson.com/	6	2014/01/01 02:29:55
8	/www.crawford.com/	4	2014/01/01 01:51:55
9	/www.price.com/	4	2014/01/01 01:07:55
10	/hernandez.com/	4	2014/01/01 01:01:55

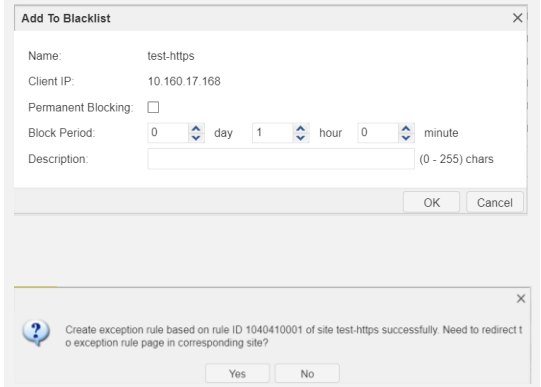
Attack Breakdown





Threat Control

Severity	Action	Details	Status Code	Capture Packets	Parameter
Critical	Block	Block Once	403	☑	
Critical	Block	Block Once	403	☑	
Critical	Block	Block Once	403	☑	
Critical	Block	Block Once	403	☑	
Critical	Block	Block Once	403	☑	
Critical	Block	Block Once	403	☑	



Full-screen Dashboard for Security Posture

Web Application Security Monitoring

Threat Distribution

Risky Site Statistics

Site Performance

Site Requests Statistics

Top Threat Intelligence

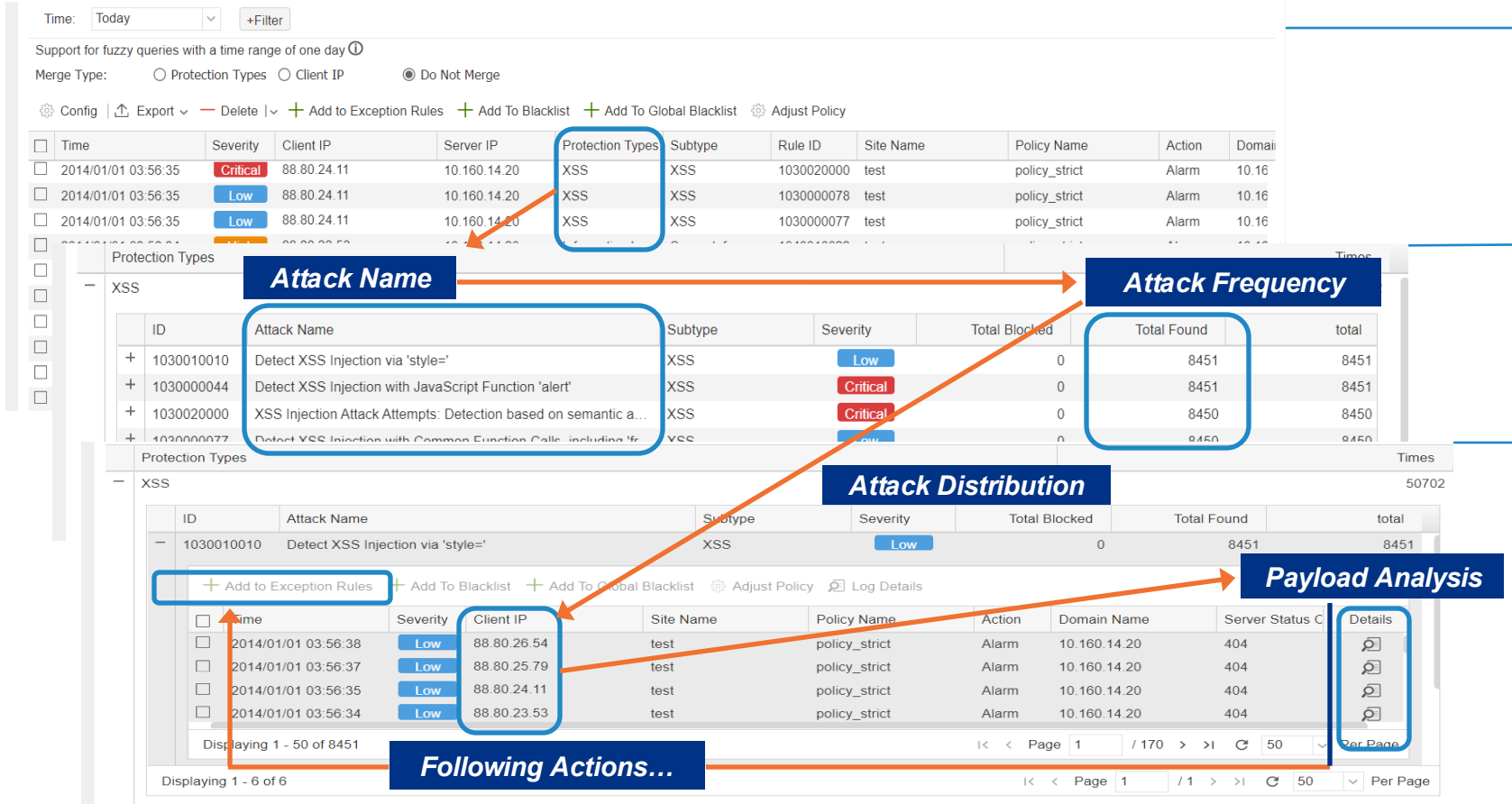
New Threat Intelligence

Risky Site Ranking

Latest Site Threat Statistics

Threat Event Type

Aggregated Logs Help to Eliminate False Positives



Original log

Aggregated log according to attack type

Aggregated log according to rule id

How to find false positives among the massive logs?
Hillstone WAF support multi-dimensional log aggregation and help admins to review log, find false positives, and tune the policy.

Informative Reporting

Report Overview

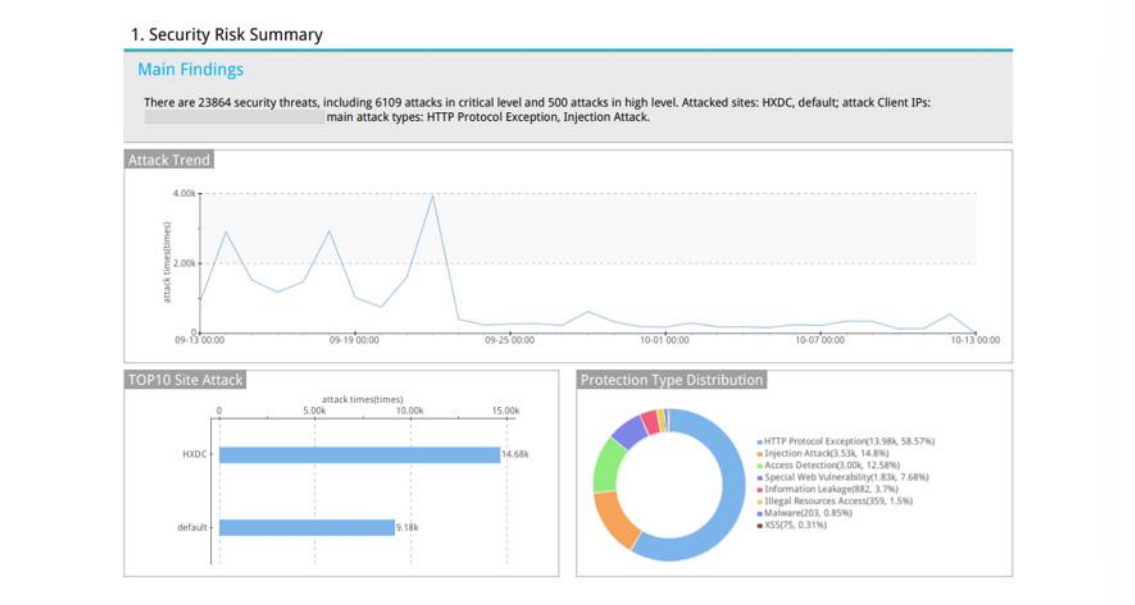
- List all reports
- Support export report in PDF/HTML/Word format
- Support manual export for customizable queries

Report Task

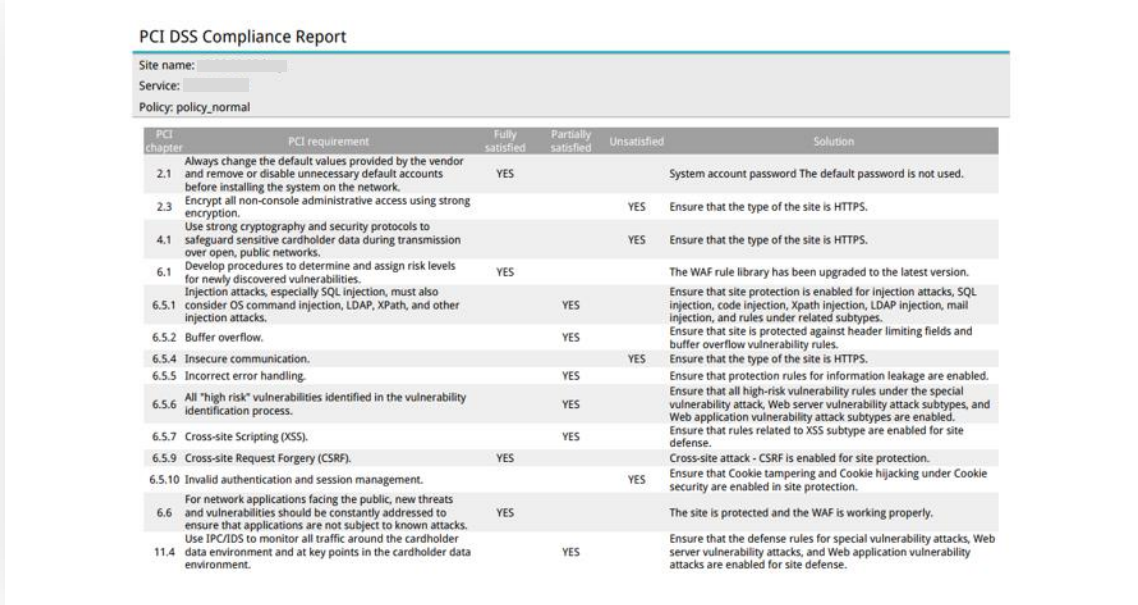
- Generate reports on-demand or on a schedule
- Send reports via FTP or email

Report Template

- Multiple pre-defined templates:
  PCI DSS compliance / site and risk assessment / site access and web traffic
- Customizable templates



A page of summary report



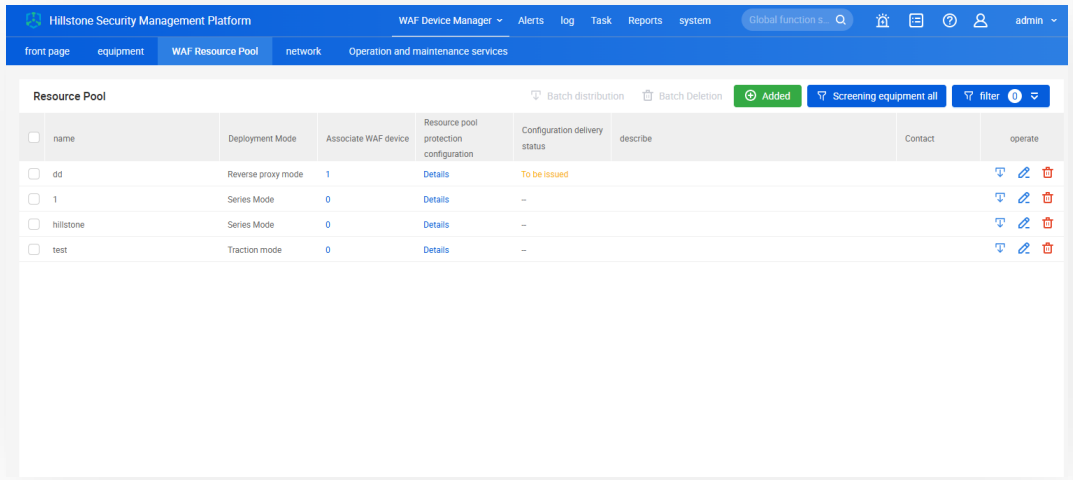
PCI chapter	PCI requirement	Fully satisfied	Partially satisfied	Unsatisfied	Solution
2.1	Always change the default values provided by the vendor and remove or disable unnecessary default accounts before installing the system on the network.	YES			System account password The default password is not used.
2.3	Encrypt all non-console administrative access using strong encryption.			YES	Ensure that the type of the site is HTTPS.
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.			YES	Ensure that the type of the site is HTTPS.
6.1	Develop procedures to determine and assign risk levels for newly discovered vulnerabilities.	YES			The WAF rule library has been upgraded to the latest version.
6.5.1	Injection attacks, especially SQL injection, must also consider OS command injection, LDAP, XPath, and other injection attacks.		YES		Ensure that site protection is enabled for injection attacks, SQL injection, code injection, Xpath injection, LDAP injection, mail injection, and rules under related subtypes.
6.5.2	Buffer overflow.		YES		Ensure that site is protected against header limiting fields and buffer overflow vulnerability rules.
6.5.4	Insecure communication.			YES	Ensure that the type of the site is HTTPS.
6.5.5	Incorrect error handling.		YES		Ensure that protection rules for information leakage are enabled.
6.5.6	All "high risk" vulnerabilities identified in the vulnerability identification process.		YES		Ensure that all high-risk vulnerability rules under the special vulnerability attack, Web server vulnerability attack subtypes, and Web application vulnerability attack subtypes are enabled.
6.5.7	Cross-site Scripting (XSS).		YES		Ensure that rules related to XSS subtype are enabled for site defense.
6.5.9	Cross-site Request Forgery (CSRF).	YES			Cross-site attack - CSRF is enabled for site protection.
6.5.10	Invalid authentication and session management.			YES	Ensure that Cookie tampering and Cookie hijacking under Cookie security are enabled in site protection.
6.6	For network applications facing the public, new threats and vulnerabilities should be constantly addressed to ensure that applications are not subject to known attacks.	YES			The site is protected and the WAF is working properly.
11.4	Use IPC/IDS to monitor all traffic around the cardholder data environment and at key points in the cardholder data environment.		YES		Ensure that the defense rules for special vulnerability attacks, Web server vulnerability attacks, and Web application vulnerability attacks are enabled for site defense.

PCI DSS Compliance Report

Centralized WAF Management with HSM

WAF Resource Pool

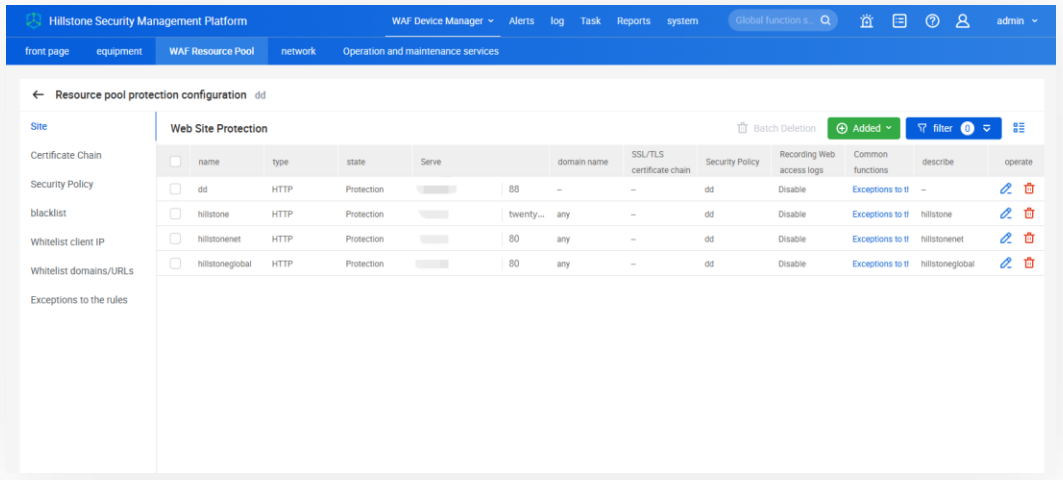
- Horizontal resource scaling for improved WAF performance
- Centralized WAF resource management integrated into Hillstone Security Management (HSM) for streamlined operations



HSM WAF Manager: WAF Resource Pool

Centralized WAF Policy and Site Management

- Add / configure site
- WAF policy configuration/ allow list / block list /exception



HSM WAF Manager: WAF Resource Pool Policy and Site Configuration

WAF Hardware Appliance Feature Highlights

High performance application layer throughput

01 Multiple models covering extensive scenarios
Hardware HTTP throughput: 600Mbps~13 Gbps

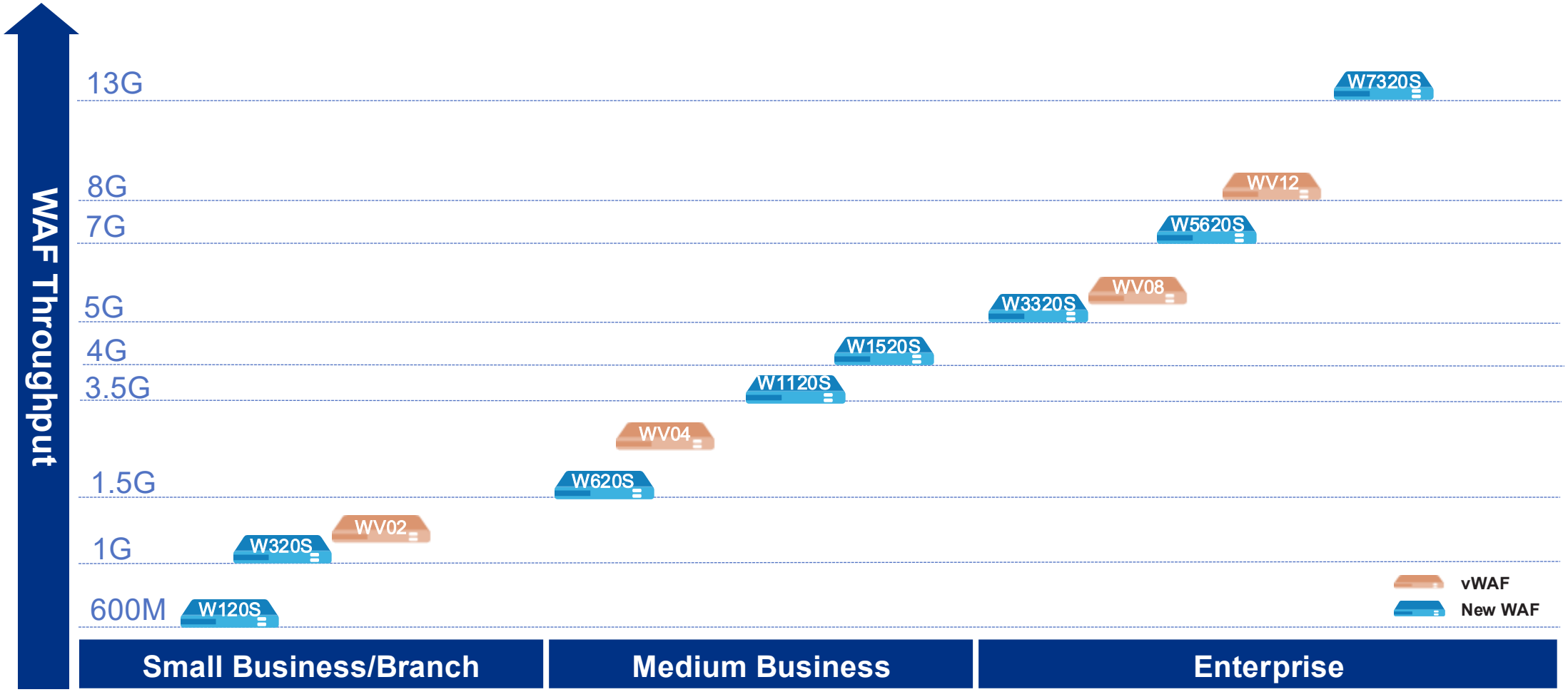
02 Flexible interface expansion options

03 SSL hardware acceleration

04 High-density interface with 1U form factor
High-end model fixed I/O Ports : 2 x QSFP+, 16 x SFP+, 8 x GE(including 4 bypass pair)

Model Selection& Ordering Information

Hillstone W-Series Web Application Firewall Portfolio



Hillstone WAF Specification

Model	W120S-IN	W320S-IN	W620S-IN	W1120S-IN	W1520S-IN	W3320S-IN	W5620S-IN	W7320S-IN
Maximum Throughput (1518 bytes) (1)	2.4G	4.5G	13G	26G	26G	40G	55G	87G
Maximum Concurrent Sessions (1)	400,000	400,000	750,000	2,500,000	2,500,000	5,000,000	5,000,000	12,000,000
Throughput Reference for Model Selection (1)	800Mbps	1.5Gbps	4.3Gbps	8.5Gbps	8.5Gbps	13.3Gbps	18.3Gbps	29Gbps
HTTP Throughput (2)	600Mbps	1Gbps	1.5Gbps	3.5Gbps	4Gbps	5Gbps	7Gbps	13Gbps
HTTP Concurrent Sessions (2)	200,000	300,000	600,000	1,500,000	1,700,000	3,000,000	3,500,000	8,000,000
HTTP New Sessions/s (2)	1,600	3,500	5,000	8,000	10,000	14,000	22,000	45,000
HTTP Maximum Transactions Per Second (TPS) (2)	2400	5,500	7,000	10,000	15,000	22,000	33,500	70,000
HTTP Throughput Reference for Model Selection (2)	100Mbps	200Mbps	400Mbps	400-1000Mbps	400-1000Mbps	1000-1500Mbps	1200-2000Mbps	2000-3000Mbps
HTTPS Throughput (without/with hardware acceleration)(3)	350Mbps/400Mbps	800Mbps/900Mbps	1.2Gbps/1.5Gbps	2Gbps/2Gbps	2.4Gbps/2.4Gbps	3.4Gbps/3.7Gbps	5 Gbps/6Gbps	10 Gbps/11 Gbps
HTTPS New Sessions/s (without/with hardware acceleration)(3)	200/500	500/1200	500/1700	1300/3500	1500/4000	2000/6000	3,500/10,000	7500/21,000
HTTPS Maximum Transactions Per Second (TPS)(without/with hardware acceleration)(3)	1500/1800	4000/4500	5000/5000	12,000/12,000	14,000/14,000	20,000/20,000	32,000/33,500	70,000/70,000
HTTPS Throughput Reference for Model Selection (without/with hardware acceleration)(3)	30Mbps	80Mbps	100Mbps	100-200Mbps	100-200Mbps	300Mbps	500Mbps	800Mbps

Notes:
(1) Network performance is obtained under WAF disabled, and no protection site configured;
(2) HTTP protection performances are obtained under protection site configured and “Medium Protection Strategy” used;
(3) HTTPS protection performances are obtained under “Medium protection strategy”, TLSv1.2 cipher suite AES128-GCM-SHA256, key length 2K RSA.

Hillstone WAF Specification(continued)

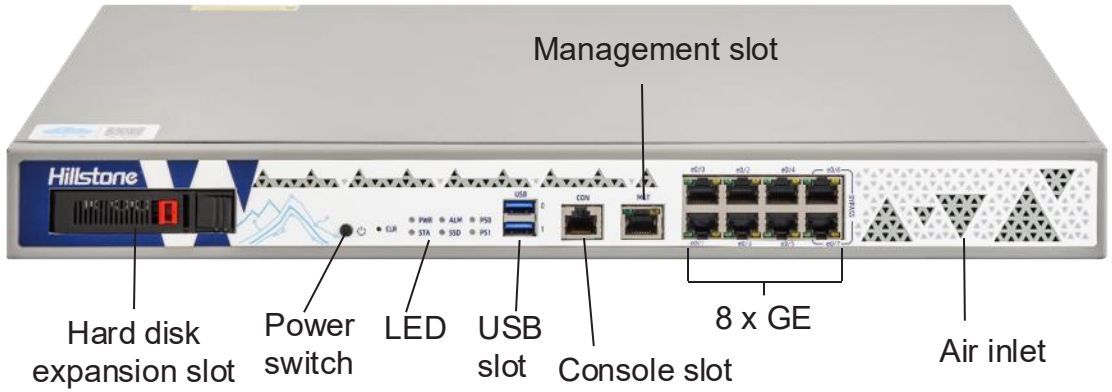
Model	W120S-IN	W320S-IN	W620S-IN	W1120S-IN	W1520S-IN	W3320S-IN	W5620S-IN	W7320S-IN
Storage	480G SSD	480G SSD	480G SSD	480G SSD	480G SSD	960G SSD	960G SSD	960G SSD
RAM	4G	4G	8G	16G	16G	32G	32G	64G
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports(SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports(SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SFP+)
Fixed I/O Ports	8 x GE(including 1 bypass pair)	8 x GE(including 1 bypass pair)	2 x SFP+, 8 x SFP, 16 x GE(including 2 bypass pairs)	2 x SFP+, 8 x SFP, 16 x GE(including 2 bypass pairs)	2 x SFP+, 8 x SFP, 16 x GE(including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE(including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE(including 2 bypass pairs)	2 x QSFP+, 16 x SFP+, 8 x GE(including 4 bypass pairs)
Available Slots for Expansion Modules	N/A	N/A	N/A	1	1	1	1	1
Expansion Module Option	N/A	N/A	N/A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Protected Site Numbers	64	64	256	512	512	1024	1024	2048
Global Site Services Can Be Protected	512	512	1024	4096	4096	8192	8192	32768
Power Specification	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC	100W, Dual AC	280W, Dual AC	280W, Dual AC	300W, Dual AC
Form Factor	1U	1U	1U	1U	1U	1U	1U	1U

Hillstone vWAF Specifications

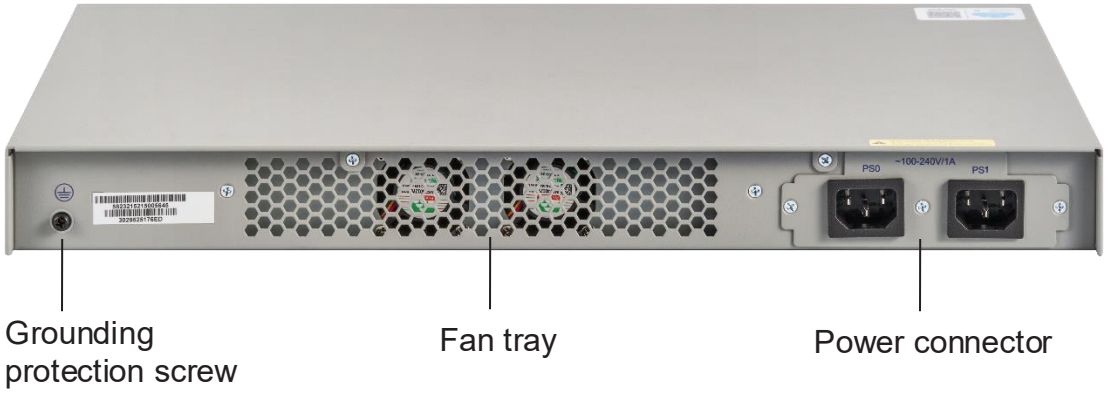
Specifications		SG-6000-WV02-IN	SG-6000-WV04-IN	SG-6000-WV08-IN	SG-6000-WV12-IN
Hardware	• CPU	2 Core	4 Core	8 Core	12Core
	• Hard Disk （min, max）	100GB, 1TB	100GB, 1TB	100GB, 1TB	100GB, 1TB
	• RAM	4GB	8GB	16G	24G
Interface	• Interface （max）	10	10	10	10
Sites	• Protection Site Numbers	64	256	512	512
	• Global Site Services Can Be Protected	256	512	8192	8192
Network Performance (Without WAF)	• Throughput（1518 Bytes） （SR-IOV enabled）	5G	10G	20G	40G
	• Concurrent Sessions	0.4M	1.2M	2.5M	4M
HTTP Protection Performance （Use “Medium policy"）	• HTTP Throughput （HTTP GET 512KByte file）	1.2G	2.5G	5.5G	8G
	• HTTP Concurrent Sessions （HTTP GET 64Byte file）	100K	300K	1.5M	2.5M
	• HTTP Connection/s （HTTP GET 1Byte file）	2,800	5,800	14,000	20,000
	• HTTP Transaction/s（TPS）	3,000	6,500	16,000	22,000
	• HTTP Model Selection Suggestion	120M HTTP Traffic	250M HTTP Traffic	550M HTTP Traffic	800M HTTP Traffic
HTTPS Protection Performance （Use “Medium policy, TLSv1.2 AES128-GCM-SHA256, 2K RSA）	• HTTPS Throughput	200M	400M	900M	1500M
	• HTTPS New Connection	400	900	2200	3300
	• HTTPS Transaction/s（TPS）	3000	6000	15000	24000
	• HTTPS Model Selection Suggestion	10M HTTPS Traffic	20M HTTPS Traffic	45M HTTPS Traffic	75M HTTPS Traffic

W120S & W320S

Front View



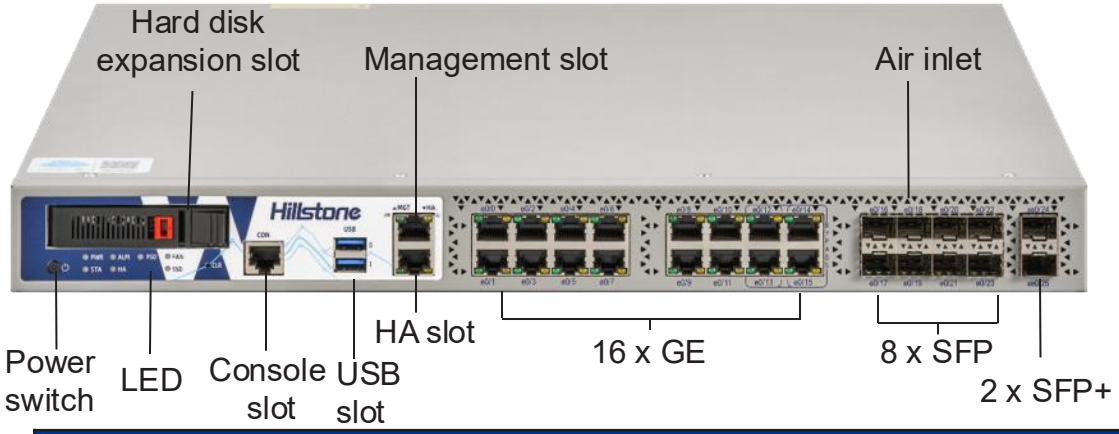
Back View



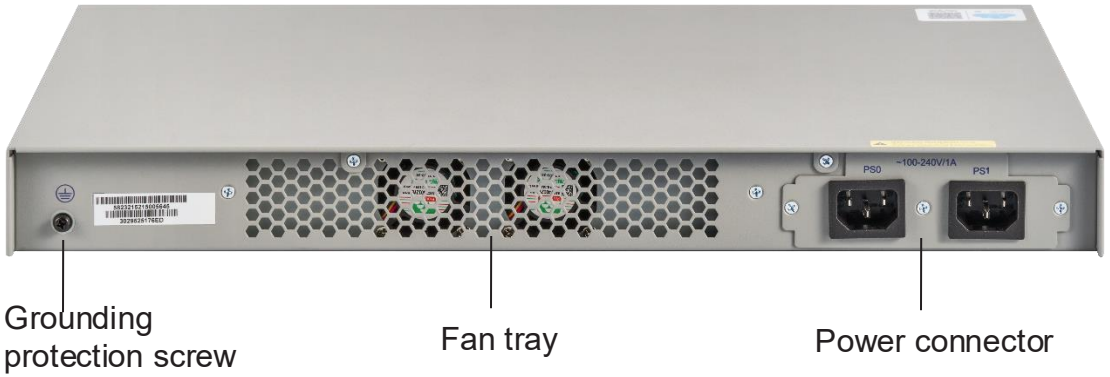
Model	W120S-IN	W320S-IN
HTTP Throughput	600Mbps	1Gbps
HTTP New Sessions/s	1,600	3,500
HTTP Maximum Transactions Per Second (TPS)	2400	5,500
HTTP Throughput Reference for Model Selection	100Mbps	200Mbps
HTTPS Throughput (without/with hardware acceleration)	350Mbps/400Mbps	800Mbps/900Mbps
HTTPS New Sessions/s (without/with hardware acceleration)	200/500	500/1200
HTTPS Maximum Transactions Per Second (TPS)(without/with hardware acceleration)	1500/1800	4000/4500
HTTPS Throughput Reference for Model Selection (without/with hardware acceleration)	30Mbps	80Mbps
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port
Fixed I/O Ports	8 x GE(including 1 bypass pair)	8 x GE(including 1 bypass pair)
Protected Site Numbers	64	64
Global Site Services Can Be Protected	512	512

W620S

Front View



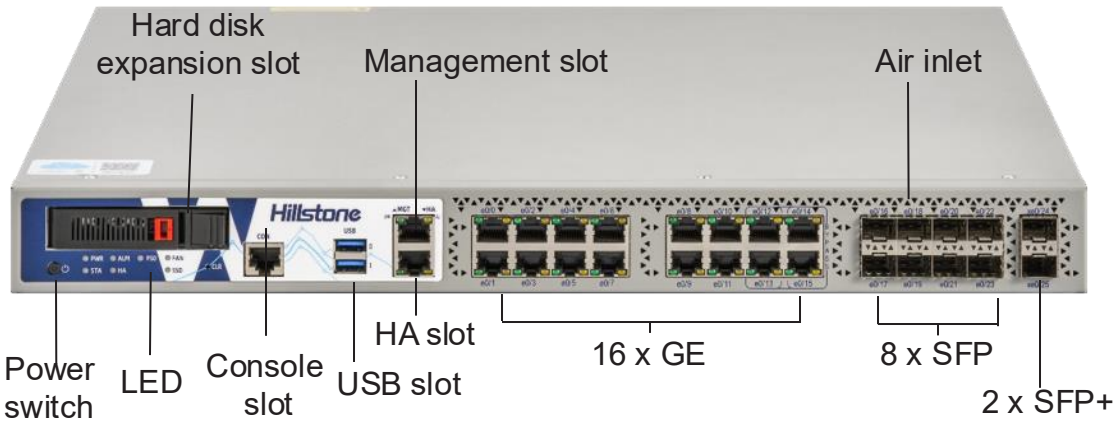
Back View



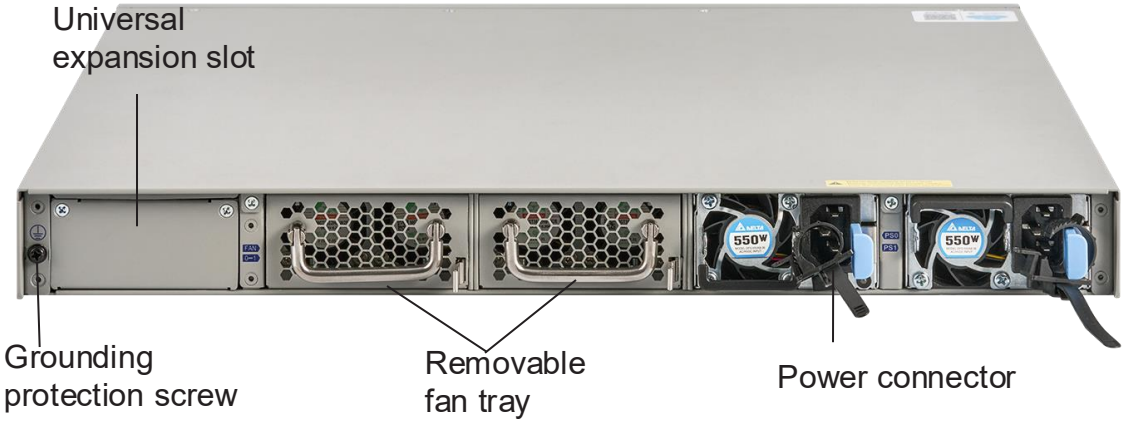
Model	W620S-IN
HTTP Throughput	1.5Gbps
HTTP New Sessions/s	5,000
HTTP Maximum Transactions Per Second (TPS)	7,000
HTTP Throughput Reference for Model Selection	400Mbps
HTTPS Throughput (without/with hardware acceleration)	1.2Gbps/1.5Gbps
HTTPS New Sessions/s (without/with hardware acceleration)	500/1700
HTTPS Maximum Transactions Per Second (TPS)(without/with hardware acceleration)	5000/5000
HTTPS Throughput Reference for Model Selection (without/with hardware acceleration)	100Mbps
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SPF)
Fixed I/O Ports	2 x SFP+, 8 x SFP, 16 x GE(including 2 bypass pairs)
Protected Site Numbers	256
Global Site Services Can Be Protected	1024

W1120S & W1520S

Front View



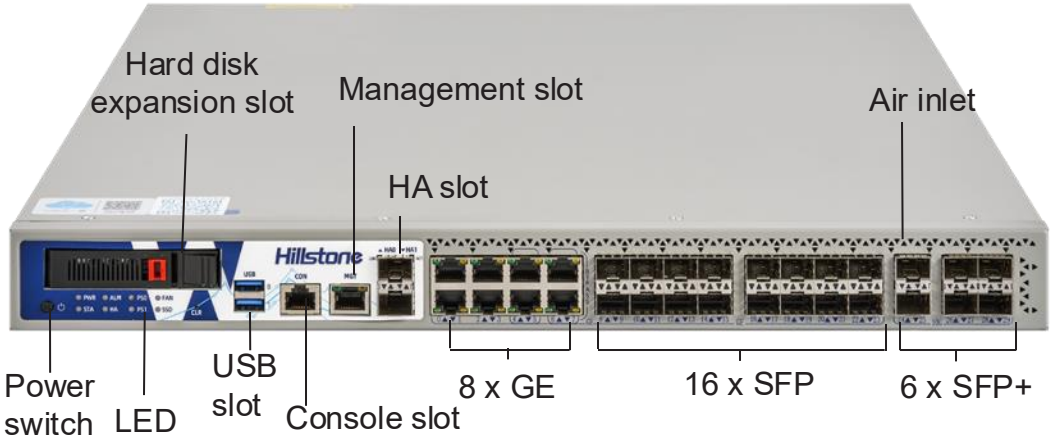
Back View



Model	W1120S-IN	W1520S-IN
HTTP Throughput	3.5Gbps	4Gbps
HTTP New Sessions/s	8,000	10,000
HTTP Maximum Transactions Per Second (TPS)	10,000	15,000
HTTP Throughput Reference for Model Selection	400-1000Mbps	400-1000Mbps
HTTPS Throughput (without/with hardware acceleration)	2Gbps/2Gbps	2.4Gbps/2.4Gbps
HTTPS New Sessions/s (without/with hardware acceleration)	1300/3500	1500/4000
HTTPS Maximum Transactions Per Second (TPS)(without/with hardware acceleration)	12,000/12,000	14,000/14,000
HTTPS Throughput Reference for Model Selection (without/with hardware acceleration)	100-200Mbps	100-200Mbps
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SPF)
Fixed I/O Ports	2 x SFP+, 8 x SFP, 16 x GE(including 2 bypass pairs)	2 x SFP+, 8 x SFP, 16 x GE(including 2 bypass pairs)
Protected Site Numbers	512	512
Global Site Services Can Be Protected	4096	4096

W3320S & W5620S

Front View

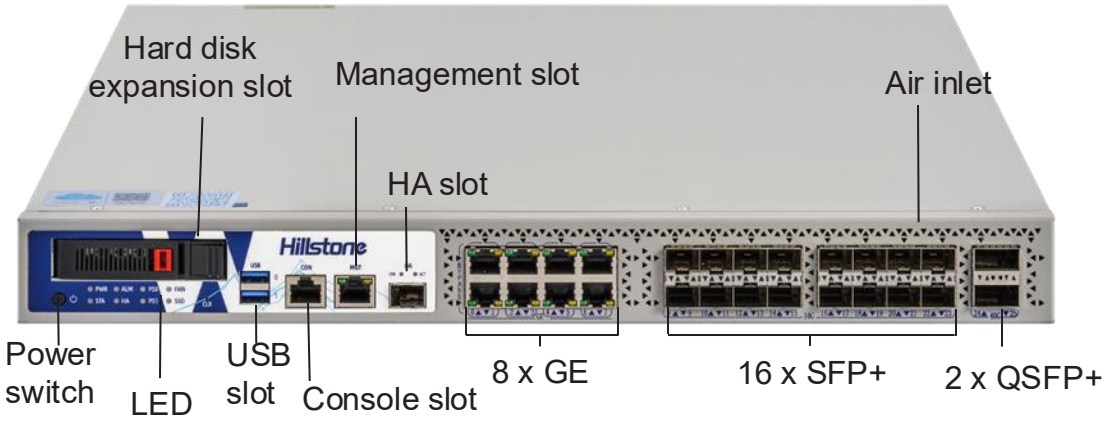


Back View

Model	W3320S-IN	W5620S-IN
HTTP Throughput	5Gbps	7Gbps
HTTP New Sessions/s	14,000	22,000
HTTP Maximum Transactions Per Second (TPS)	22,000	33,500
HTTP Throughput Reference for Model Selection	1000-1500Mbps	1200-2000Mbps
HTTPS Throughput (without/with hardware acceleration)	3.4Gbps/3.7Gbps	5 Gbps/6Gbps
HTTPS New Sessions/s (without/with hardware acceleration)	2000/6000	3,500/10,000
HTTPS Maximum Transactions Per Second (TPS)(without/with hardware acceleration)	20,000/20,000	32,000/33,500
HTTPS Throughput Reference for Model Selection (without/with hardware acceleration)	300Mbps	500Mbps
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports(SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports(SFP+)
Fixed I/O Ports	6 x SFP+, 16 x SFP, 8 x GE(including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE(including 2 bypass pairs)
Protected Site Numbers	1024	1024
Global Site Services Can Be Protected	8192	8192

W7320S

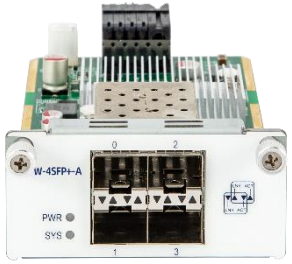
Front View

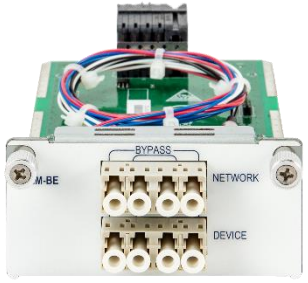


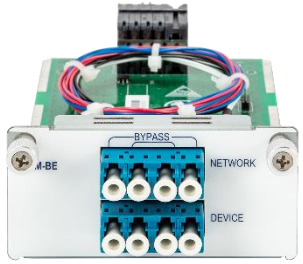
Back View

Model	W7320S-IN
HTTP Throughput	13Gbps
HTTP New Sessions/s	45,000
HTTP Maximum Transactions Per Second (TPS)	70,000
HTTP Throughput Reference for Model Selection	2000-3000Mbps
HTTPS Throughput (without/with hardware acceleration)	10 Gbps/11 Gbps
HTTPS New Sessions/s (without/with hardware acceleration)	7500/21,000
HTTPS Maximum Transactions Per Second (TPS)(without/with hardware acceleration)	70,000/70,000
HTTPS Throughput Reference for Model Selection (without/with hardware acceleration)	800Mbps
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port(SFP+)
Fixed I/O Ports	2 x QSFP+, 16 x SFP+, 8 x GE(including 4 bypass pairs)
Protected Site Numbers	2048
Global Site Services Can Be Protected	32768

Expansion Module







Module	IOC-W-4SFP+-A-IN	IOC-W-2QSFP+-A-IN	IOC-W-2MM-BE-A-IN	IOC-W-2SM-BE-A-IN
I/O Ports	4 x SFP+ Ports	2 x QSFP+ Ports	MM Bypass (2 pairs of bypass ports)	SM Bypass (2 pairs of bypass ports)
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)
Applicable Model	W1120S/W1520S / W3320S / W5620S / W7320S			

WAF Ordering Guide

Category	SKU	Definition	Term
Base System	SG-6000-W120S/W320S/W620S/W1120S/W1520S/W3320S/W5620S/W7320S-IN-yy	HW & SW w/ HW warranty, SW update services and WAF signature database upgrade	1-5 yrs. (yy:12/24/36/48/60)
Renewal Service-Software	SGSV-W120S/W320S/W620S/W1120S/W1520S/W3320S/W5620S/W7320S-IN-yy-SU	In-warranty software renewal service	1-3 yrs. (yy:12/24/36)
Renewal Service-Hardware	• SGSV-W120S/W320S/W620S/W1120S/W1520S/W3320S/W5620S/W7320S-XthY-HU	• 2nd-10th yr. basic in-warranty hardware renewal service(applicable to renewal before warranty expires);	• 1 yr.(from 2nd-10th yr.)(XthY: 2nd Y/3RDY/4th Y/5th Y/6th Y/7th Y/8thY/9th Y/10thY)
	• SGSV-W120S/W320S/W620S/W1120S/W1520S/W3320S/W5620S/W7320S-IN-12-HR	• 1 yr. basic hardware warranty(applicable to renewal after warranty expires)	• 12mons.
IP Reputation	IPR-W120S/W320S/W620S/W1120S/W1520S/W3320S/W5620S/W7320S-IN-yy	IP Reputation subscription service	1-5 yrs. (yy:12/24/36/48/60)
SSL	SSL-W120S/W320S/W620S/W1120S/W1520S/W3320S/W5620S/W7320S-IN	SSL hardware acceleration license	N/A
Others	• IOC-W-4SFP+-A-IN-yy • MCSV-IOC-W-2QSFP+-A-IN-yy-U • MCSV-IOC-W-2MM-BE-A-IN-12-R	• 4xSFP+ I/O interface module with HW warranty • Warranty for 2xQSFP+ I/O interface module (applicable to renewal before warranty expires) • Warranty for Multi-mode bypass module(applicable to renewal after warranty expires)	• 1-5 yrs. (yy:12/24/36/48/60) • 1-3 yrs. for in-warranty renewal(yy:12/24/36) • 12mons. for out-of-warranty renewal

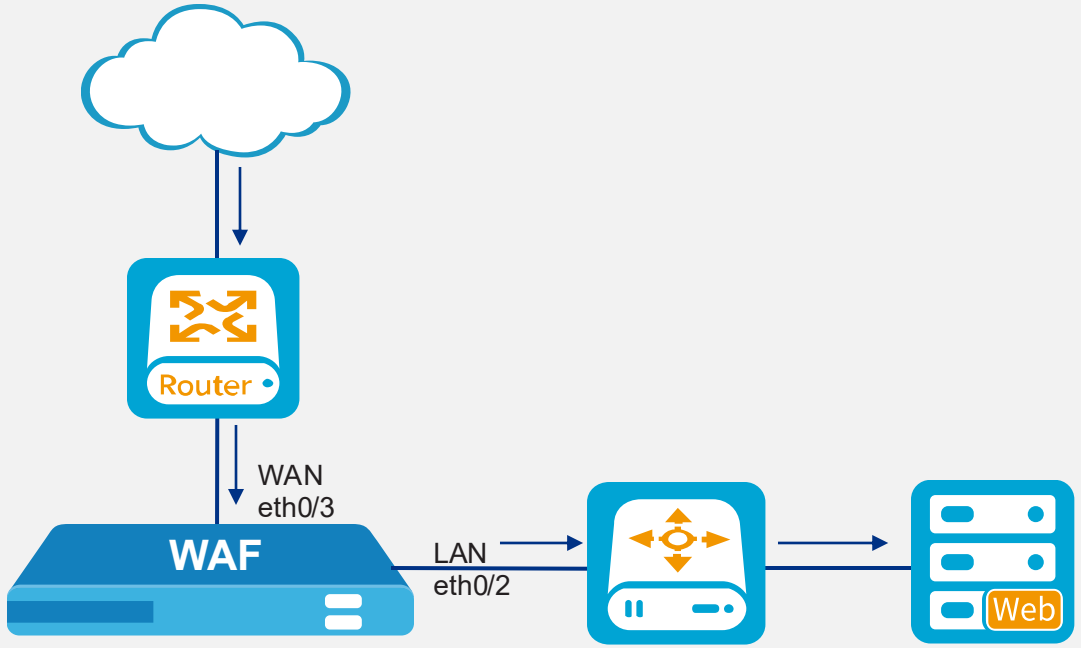
vWAF Ordering Guide

Category(Perpetual Mode)	SKU	Definition	Term
Base System	SG-6000-WV02/WV04/WV08/WV12-BP-IN	vWAF Perpetual License Base System	N/A
Maintenance Service	SG-6000-WV02/WV04/WV08/WV12-SP-IN-yy	vWAF software base system with software upgrade services	1-5 yrs. (yy:12/24/36/48/60)
IP Reputation License	IPR-WV02/WV04/WV08/WV12-IN-yy	vWAF IP Reputation Subscription	1-5 yrs. (yy:12/24/36/48/60)

Category(Subscription Mode)	SKU	Definition	Term
Base System	SG-6000-WV02-SS-IN-yy	vWAF Subscription Package including identify database upgrade and software upgrade services	1 mon. or 12 mons.(yy:1/12)
IP Reputation License	IPR-WV02-SS-IN-yy	vWAF IP Reputation Subscription	1 mon. or 12 mon.(yy:1/12)

Deployment Modes& Use Cases

Transparent Proxy/Transparent Inspection Mode



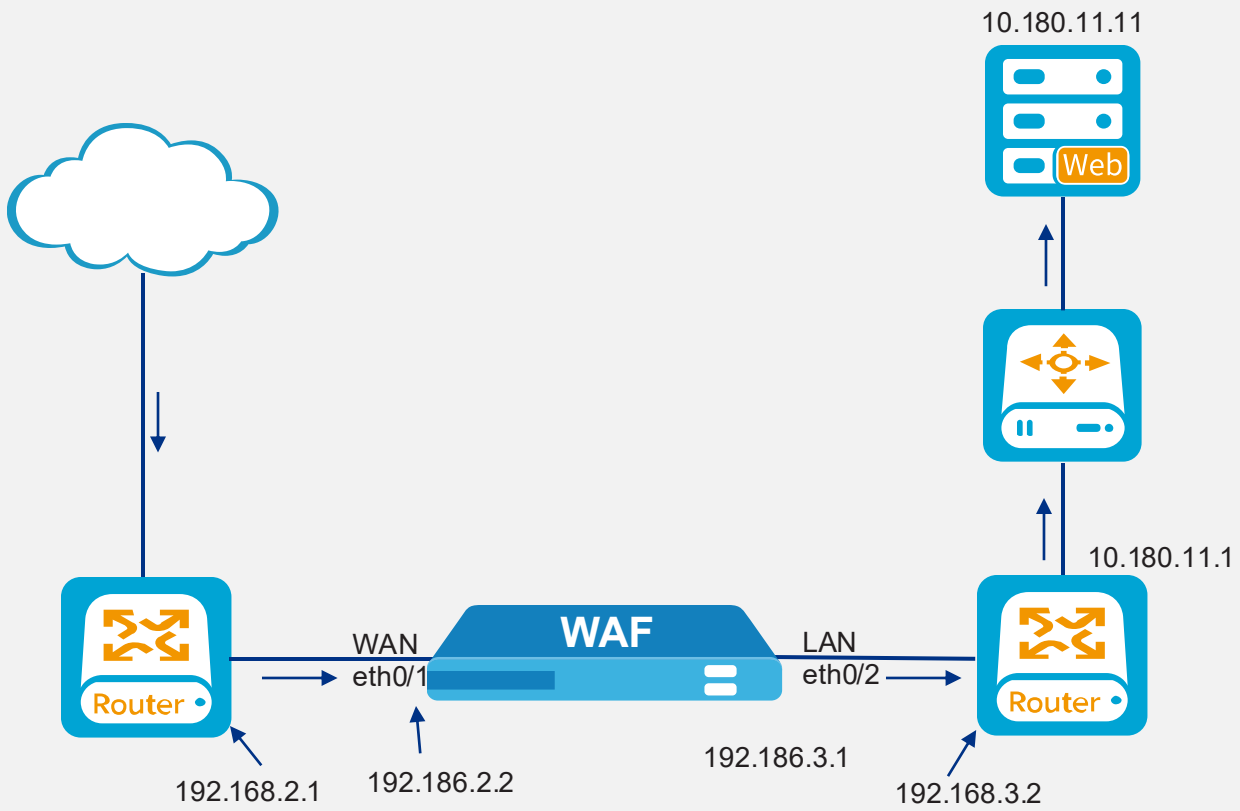
Deployment

- Layer 2 deployment
- Deployed inline between clients and servers

Pros

- Easy to deploy, plug and play
- In transparent inspection mode, WAF supports security check on MPLS traffic

Reverse Proxy Mode



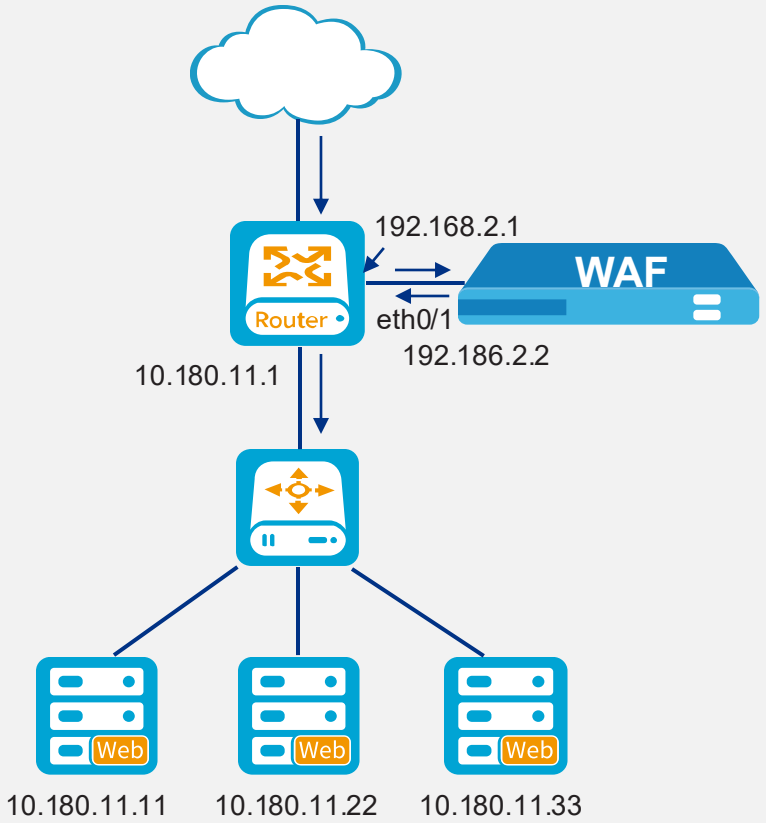
Deployment

- Layer 3 deployment
- Deployed inline between clients and servers

Pros

- Support server load balancing
- IP are not exposed to clients

One-arm Reverse Proxy Mode



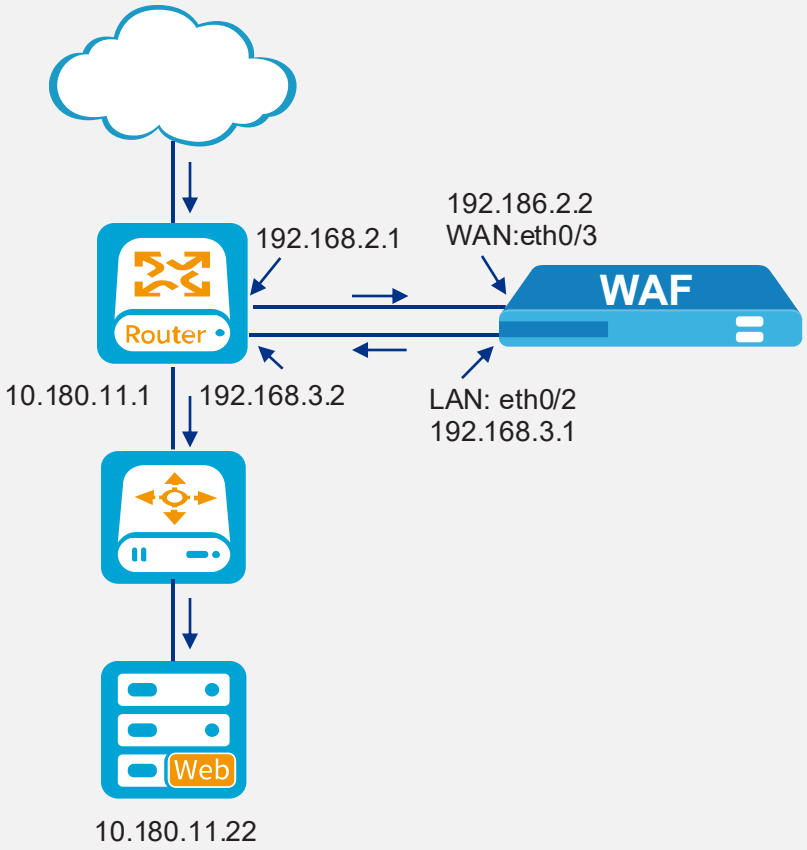
Deployment

- Layer 3 deployment
- Single interface for traffic in and out

Pros

- Support server load balancing
- IP are Not exposed to clients
- No impact to existing network deployment

Traction Proxy Mode



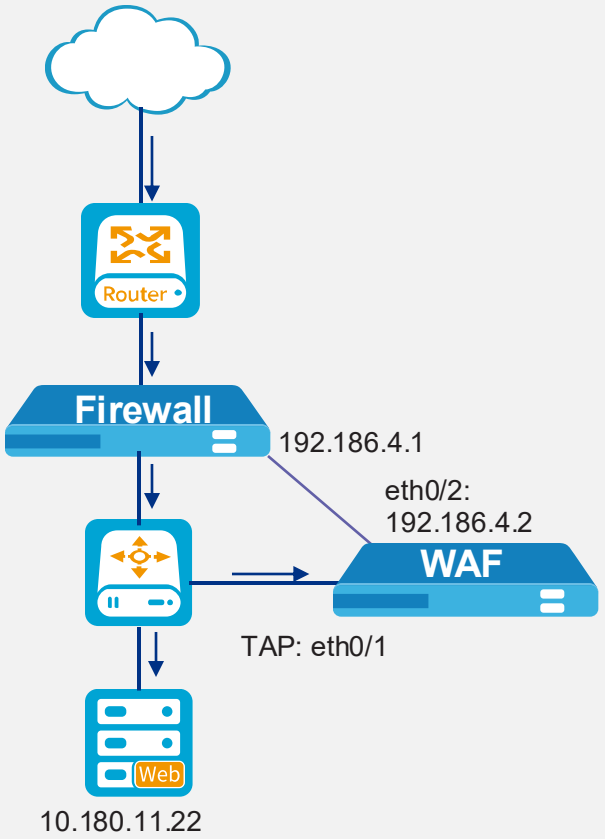
Deployment

- Layer 3 deployment
- Requires two interfaces: one in and one out
- Requires the router to redirect the traffic from clients to WAF and then from WAF back to servers.

Pros

- Auto failover without bypass

TAP Mode



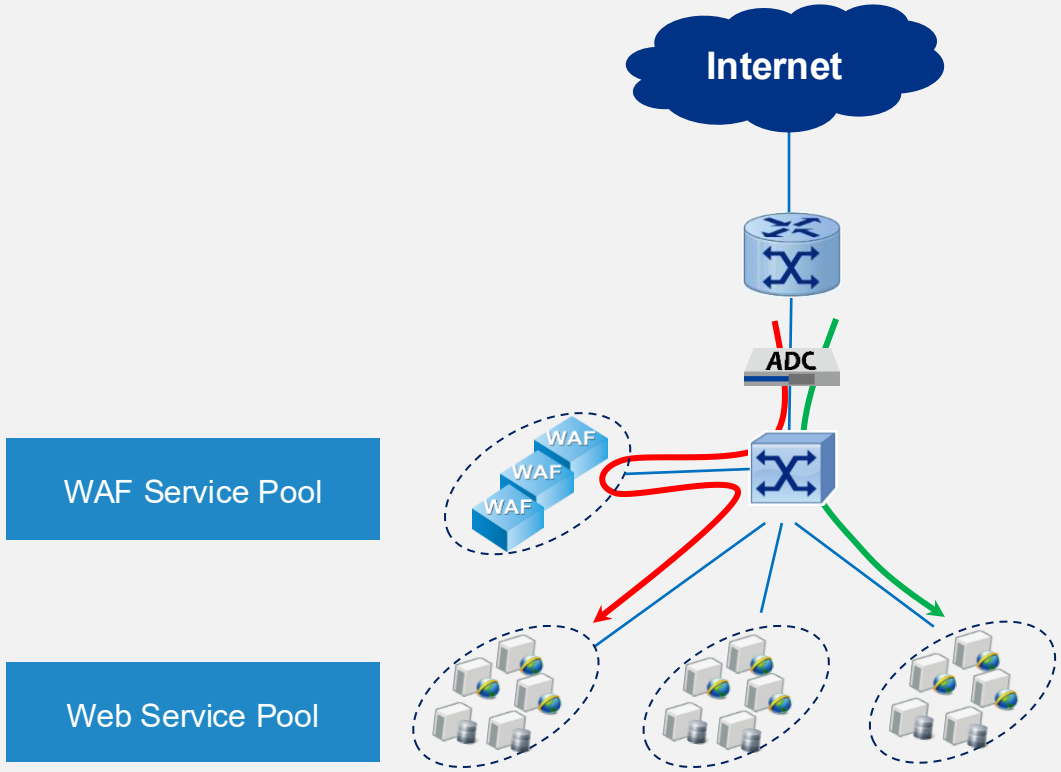
Deployment

- Layer 2 deployment
- Traffic are mirrored to WAF
- WAF analyzes the behavior of the traffic for detection
- WAF does NOT forward traffic back to the network
- WAF updates block list to NGFW if it finds the source IP of an attack
- Support attack mitigation

Pros

- No impact to existing network deployment

Hillstone ADC Provides Scalability for WAF



Challenge

- Performance of single WAF appliance maybe not enough for heavy traffics
- WAFaaS

Solutions

- With the help of Hillstone ADC, WAF can expands its protection performance for high-traffic web protection scenario.
- Service pool with multiple vWAF.

Use Case 1: Government Agencies

Challenge

- **Sensitive Data Protection:** Government agencies have to follow all regulatory and compliance requirements, especially data privacy and sensitive data protection.
- **Critical Infrastructures Protection:** Protecting critical infrastructures, such as energy, transport, healthcare or emergency services, from DDoS attacks and ensuring 24x7 uptime is a top priority for governments.
- **Malicious Defacement:** The government website is the external image of government agencies, once the government website is attacked and cannot provide services to the public or the website pages are defaced, the impact would be huge.

Solutions

- Hillstone WAF can secure business-critical web applications and sensitive information protection from the OWASP Top 10, such as sensitive data exposure, Cross Site Scripting (XSS) , etc., helping government agencies protect sensitive data and prevent leakage.
- Hillstone WAF is architected to defend public-facing websites, applications, APIs, infrastructure, against different types of DDoS attacks.
- Hillstone WAF supports Anti-Defacement for dynamic and static contents, meanwhile it's also able to disconnect with one click, protecting users from reputation damage and data breaches.

Use Case 2: Finance Industry

Challenge

- **Business Continuity:** Threats and disruptions mean a loss of revenue and higher costs, high business availability is an important part of financial industry and there is an especially high concern over DDoS attacks.
- **Sensitive Data Protection:** The surge in online banking along with the prospect of stricter data privacy laws is making sensitive data protection a big challenge.
- **PCI DSS Compliance:** Assessing web assets for secure configurations and maintaining effective governance of web assets and other items vital to PCI compliance can be challenging.

Solutions

- Hillstone WAF is designed to mitigate DDoS attacks targeting web applications, ensuring business continuity with guaranteed uptime. Hillstone WAF also ensures high availability by providing failover solutions for businesses to enable uninterrupted communication and improve reliability.
- Hillstone WAF uses advanced threat detection technology to prevent attacks reaching user's sensitive customer data, financial transactions, and other parts of user's ecosystem.
- Hillstone WAF continuously monitors user's website for adherence to PCI DSS compliance and generate reports according to the requirements, helping users to secure their public facing web applications.

Use Case 3: Education Industry

Challenge

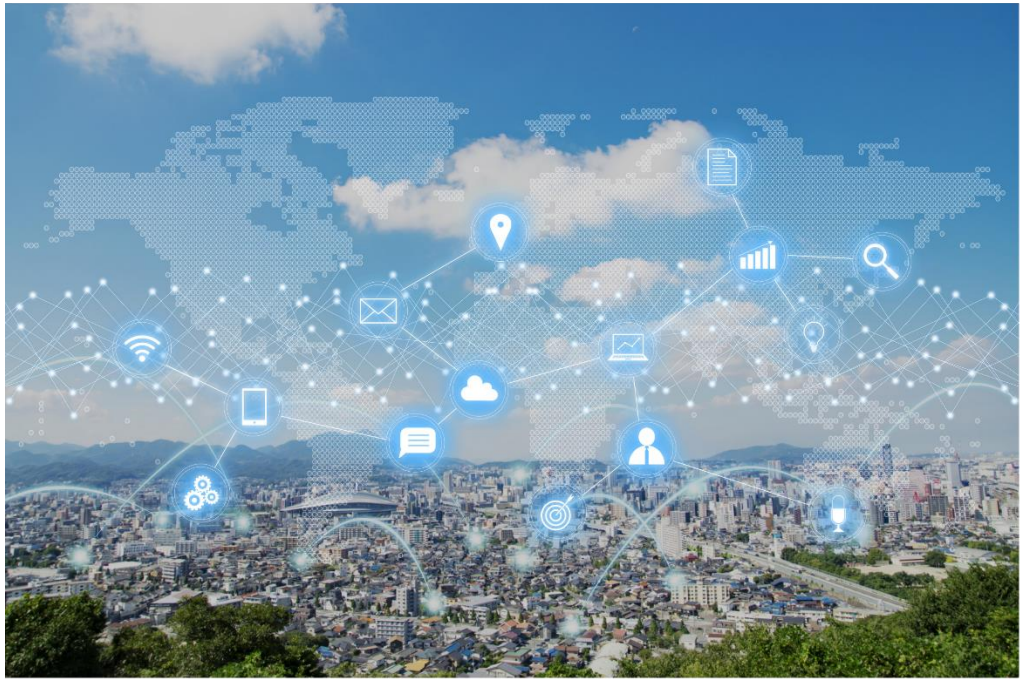
- **Student and Faculty Data Breach:** For education, data breaches are a concern as vast amount of diverse information holds on students and staff, including Personally Identifiable Information (PII), financial information, and even health information.
- **Availability of Online Service:** Schools and universities depend on their websites and online services. Networks and applications must be available 24x7 to allow students and faculty access to resources, especially during admissions, exams and other time sensitive periods.
- **Malicious Defacement:** Hackers can tamper with student grades, creating fake degrees and diplomas, etc. by exploiting web business systems vulnerabilities in portals or mailbox systems, etc.

Solutions

- Hillstone's WAF leverages machine-learning algorithms to provide comprehensive protection against DDoS, the OWASP Top 10 threats, ensuring the security of APIs and web applications accessed daily by students and faculty.
- Hillstone's WAF ensures educational institutions the availability of online services by proactively blocking DDoS traffic and attacks.
- Hillstone WAF supports Anti-Defacement for dynamic and static contents, monitoring customer's web sites for defacement attacks. Meanwhile it's also able to disconnect with one click, protecting customers from further damage.

Case Studies

Case Study 1: Protect Critical Business for a Service Provider



Customer Requirements

- The Customer requires high HTTP throughput and QPS performance.
- Dual Stacking of IPv4 and IPv6.
- Strictly low false interception rate of normal HTTP messages.
- Attack detection and protection against a variety of SQL injection attacks, credential-stuffing attacks, web shell attacks and HTTPS attacks, etc. The customer requires WAF devices to identify attack type and the detection rate should meet the corresponding standards.

Value for Customers

- Hillstone WAF provides high HTTP throughput and maximum concurrent sessions performance, which facilitates the customer to manage a high-volume traffic website.
- Hillstone WAF detects and protects against network layer security attacks(e.g. DDoS attacks, flood attacks, etc.), and also application layer security attacks(e.g. OWASP Top 10 including injection attacks, cross site scripting (XSS) attacks, etc.), which helps the customer to block unknown or malicious traffic and ensure uninterrupted access of legitimate traffic.
- Hillstone WAF integrates the industry's most innovative semantics analysis with traditional WAF detection engines. This dual-engine approach significantly improves the accuracy of detection and efficiency in operation.

Case Study 2: Protect the Cloud-Based Digital Platform Business for a National Oil Corporation

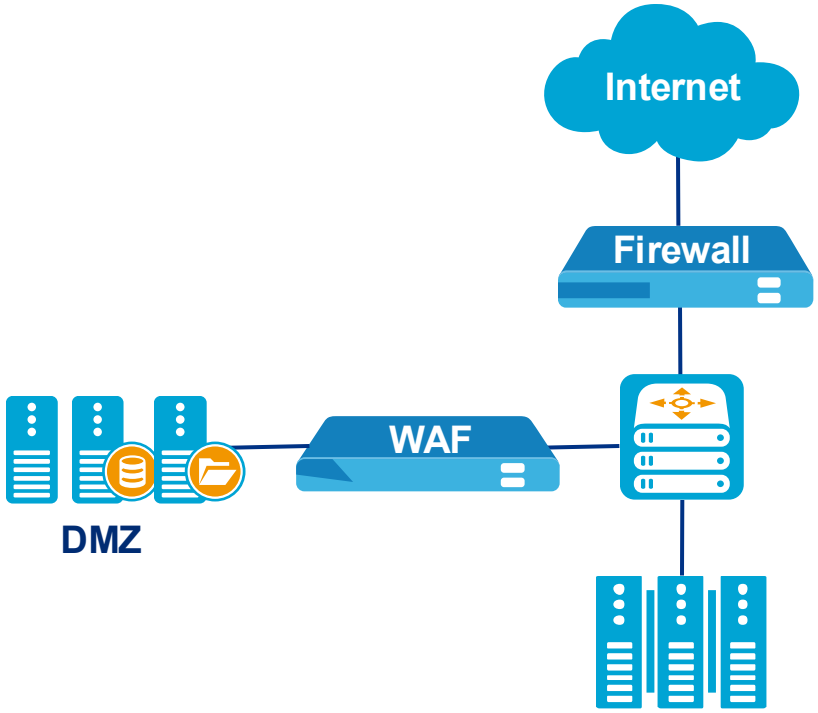
Customer Requirements

- The customer is planning to build a fully cloud-based digital platform, launching its e-commerce business as well as migrating its business systems to the cloud. To secure the transition to the cloud, the customer need effective web security protection of its digital platform.

Value for Customers

- By analyzing traffic and filtering potentially harmful and exploitable traffic, Hillstone WAF provides comprehensive security for web servers, applications and APIs, which helps the customer to safeguard their e-commerce website;
- Hillstone WAF supports site auto-discovery, which enables the customer to discover web assets in the network and add them as protected assets with one click;
- Hillstone WAF provides excellent protection against DDoS attacks, which ensures the customer uninterrupted service delivery.

Case Study 3: Protect DMZ for a Trust Fund Agency



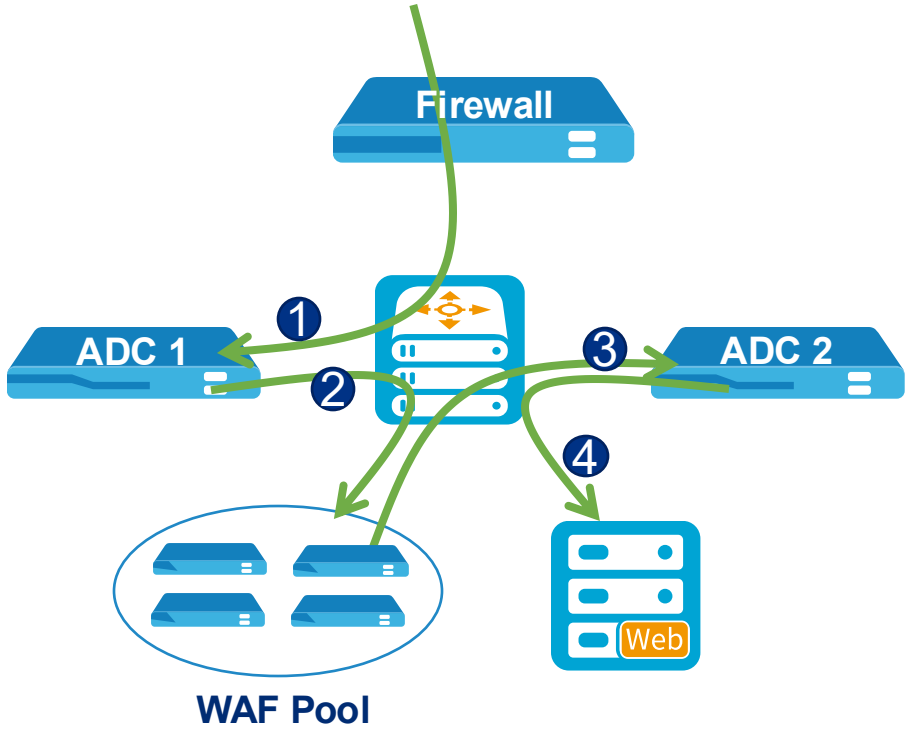
Customer Requirements

- The customer's systems are currently mostly open to the public, they need protection from external and internal attacks against their web application services;
- Vulnerabilities affect a wide range of hardware and software devices, the customer requires advanced protection against server system vulnerabilities;
- The customer needs protection against DDoS attacks;
- The customer requires the device to work without affecting normal operations during prep stage.

Value for Customers

- Hillstone WAF is deployed in the server area to effectively defend against Web attacks such as SQL injection, cross site scripting, Trojan horse attacks, malicious scanning, etc. It supports sensitive information protection, anti-defacement, application layer DDoS protection, etc., to maximize the security of website operation.
- Transparent proxy mode enables analysis and defense-in-depth security for web applications.
- Hillstone's innovative TAP mode enables WAF analyzing the mirrored traffic without affecting normal business.
- Hillstone WAF provides hide-my-site function, so hackers will not be able to view the source information of web, URL return code of Web application firewall, HTTP header information and IP of terminal server.

Case Study 4: Protect Application and Business in Web for a Fin-Tech Company



Customer Requirements

- As business migrates to the cloud and data becomes increasingly integrated, the customer is facing more risks due to the open nature of web systems. Customersin the financial industry need to adopt application security solutions to better control and protect their business and web apps.
- With the increase of the number of users and appplications, web trafiic is also growing rapidly. The customer need high-performance web application delivery capabilities, as well as the ability to dynamically expand to meet further demand.

Value for Customers

- Hillstone WAF and ADC(Application Delivery Controller) support Bypass function and HA deployment mode, which enable the application security solution to ensure high availability and business continuity.
- The upstream ADC can help WAF to build a WAF pool, expand the application security capability by adding more devices when needed.

Département Commercial

WCA

HAFS

Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY Vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision