CITRIX CLOUD SOLUTIONS — NETSCALER WAF

NetScaler WAF — Web Application Firewall for External-to-Internal Traffic

Citrix

Every web application you expose to the internet is under constant attack. SQL injection, cross-site scripting, credential stuffing, bot floods — these threats never stop. NetScaler WAF sits between the internet and your applications, inspecting every request in real time and blocking attacks before they reach your servers, without affecting legitimate users.

OWASP Top 10 — Full Protection | Learn Mode + Enforce Mode | Bot Management Built In | Included — Advanced & Premium Licence

OAS · Protect. Detect. Recover.

Prepared 11 September 2026

THE THREAT REALITY

Why Every Exposed Application Needs a WAF

Traditional network firewalls block ports and protocols. They cannot inspect what is inside an HTTPS request. Web application attacks operate entirely within legitimate traffic, on port 443, inside encrypted sessions that firewalls wave through without question. A WAF reads the content of every request and makes an intelligent decision about whether to allow or block it.

The Attack Surface

Any Application Facing the Internet

Customer portals, staff remote access, APIs, partner integrations, e-commerce, online banking — every web endpoint is a potential attack vector. Attackers probe these continuously, often using automated tools that test thousands of exploit patterns per minute. A firewall without WAF sees HTTPS and lets it through. The WAF sees what is inside.

What Network Firewalls Miss

Application-Layer Attacks Are Invisible to Port-Based Rules

SQL injection, cross-site scripting, and command injection all arrive on the same port 443 as legitimate user traffic. A traditional firewall cannot distinguish between a valid login attempt and a SQL injection payload buried in a form field. WAF inspection operates at Layer 7, reading the actual content of HTTP/HTTPS requests and applying policy logic to what it finds.

Already in Your Licence

NetScaler WAF Is a Feature You May Already Own

If your organisation is running NetScaler on an Advanced or Premium licence, the WAF capability is already included — it simply needs to be enabled and configured. OAS activates, tunes, and manages the WAF on your behalf, turning a dormant licence entitlement into active, policy-enforced protection for all your web-facing applications.

OWASP TOP 10 PROTECTION

The Ten Attack Categories NetScaler WAF Stops

The OWASP Top 10 is the globally recognised standard for web application security risk. NetScaler WAF is built to detect and block every category in this list, either through signature-based matching, behavioural analysis, or positive security model enforcement. Licence note: WAF protection for all OWASP Top 10 categories is available on NetScaler Advanced and Premium editions. If you are unsure which edition you are running, OAS can review your current entitlements and advise on the simplest path to activation.

OWASP A01 — BROKEN ACCESS CONTROL

Preventing Unauthorised Resource Access

Users accessing data or functions outside their permitted scope. Broken access control allows attackers to act as other users, access admin functions, or read files they should not see. NetScaler WAF enforces URL-level access policies, detects directory traversal attempts, and blocks requests that attempt to access restricted resources outside of defined session and authentication boundaries.

WAF POLICY + URL ACCESS CONTROL + SESSION ENFORCEMENT

OWASP A02 — CRYPTOGRAPHIC FAILURES

Protecting Sensitive Data in Transit

Weak or missing encryption exposing personal and financial data. NetScaler terminates SSL/TLS at the edge and enforces strong cipher policy, rejecting weak TLS versions, deprecated cipher suites, and insecure renegotiation. All traffic is inspected before reaching backend servers, and HTTP-to-HTTPS redirection is enforced centrally without requiring changes to individual applications.

TLS TERMINATION + CIPHER POLICY ENFORCEMENT + HTTP REDIRECT

OWASP A03 — INJECTION

Blocking SQL, Command & LDAP Injection

Attacker-controlled data interpreted as commands by the backend. SQL injection remains the most exploited web vulnerability category. NetScaler WAF inspects all inbound request parameters — URL paths, query strings, POST bodies, headers, and cookies — for injection patterns against SQL, OS commands, LDAP, and XML/XPath. Payloads are detected and blocked before they reach the application or database.

SQL INJECTION DETECTION + COMMAND INJECTION + POSITIVE SECURITY MODEL

OWASP A04 — INSECURE DESIGN

Compensating for Application-Level Design Flaws

Missing rate limits, business logic gaps, and unvalidated workflows. Where application design does not enforce rate limiting or business logic constraints, the WAF can compensate at the edge. NetScaler applies rate limiting per source IP, per user session, or per URL, preventing brute-force login attempts, credential stuffing, and automated abuse of application workflows without modifying the application itself.

RATE LIMITING + SESSION CONTROL + REQUEST THROTTLING

OWASP A05 — SECURITY MISCONFIGURATION

Masking Misconfigured Application Responses

Verbose error messages, exposed admin paths, and default credentials. Applications often return stack traces, server version banners, or sensitive path information in error responses, handing attackers a roadmap. NetScaler WAF strips these from responses before they reach users, blocks requests targeting known admin endpoints and default paths, and enforces response filtering to prevent information leakage from misconfigured backends.

RESPONSE SANITISATION + ERROR PAGE MASKING + ADMIN PATH BLOCKING

OWASP A06 — VULNERABLE & OUTDATED COMPONENTS

Virtual Patching Without Application Downtime

Known CVEs exploited before patches can be applied. When a new CVE is disclosed for a web framework, library, or CMS, organisations often cannot patch immediately. NetScaler WAF provides virtual patching, deploying a blocking rule for the exploit signature at the WAF layer, protecting the vulnerable application while the underlying patch is tested and scheduled, without requiring an emergency maintenance window.

VIRTUAL PATCHING + CVE SIGNATURE RULES + ZERO-DOWNTIME PROTECTION

OWASP A07 — IDENTIFICATION & AUTHENTICATION FAILURES

Stopping Credential Attacks at the Gateway

Brute force, credential stuffing, and session token theft. NetScaler WAF detects and blocks credential stuffing campaigns by identifying automated login patterns — too many attempts from a single IP, requests without valid browser fingerprints, or submission rates inconsistent with human behaviour. Combined with nFactor multi-step authentication, it provides a layered defence at the authentication perimeter.

CREDENTIAL STUFFING DETECTION + BOT FINGERPRINTING + NFACTOR MFA

OWASP A08 — SOFTWARE & DATA INTEGRITY FAILURES

Protecting Against Malicious Content Injection

Tampered updates, insecure deserialisation, and CI/CD pipeline attacks. NetScaler WAF validates the integrity of inbound requests, detecting serialised object payloads that indicate deserialisation attacks, enforcing form field validation to prevent tampered data from reaching application logic, and applying content-type enforcement to ensure requests match expected formats before any processing occurs.

DESERIALISATION PROTECTION + FORM FIELD VALIDATION + CONTENT-TYPE ENFORCEMENT

OWASP A09 — SECURITY LOGGING & MONITORING FAILURES

Full Visibility Into Attack Traffic

Attacks going undetected due to lack of logging and alerting. Every request inspected by NetScaler WAF generates a detailed log entry, including the source IP, request details, matched rule, and action taken. OAS integrates WAF logs into centralised monitoring, enabling real-time alerting on attack patterns, trend analysis across time periods, and compliance reporting for audit and regulatory purposes.

FULL WAF LOGGING + OAS MONITORING INTEGRATION + COMPLIANCE REPORTING

OWASP A10 — SERVER-SIDE REQUEST FORGERY (SSRF)

Blocking Internal Network Pivoting via Web Apps

Attackers using the application server to reach internal resources. SSRF allows an attacker to force a web server to make requests to internal systems — cloud metadata endpoints, internal APIs, or database servers — that should never be reachable from the internet. NetScaler WAF detects SSRF patterns in request parameters and blocks outbound calls to internal address ranges, preventing the application layer from becoming a pivot point.

SSRF PATTERN DETECTION + INTERNAL RANGE BLOCKING + OUTBOUND REQUEST POLICY

Beyond Signatures — The Positive Security Model

NetScaler WAF can operate in positive security mode, learning what normal, legitimate traffic looks like for each application and blocking anything that deviates from that profile. This catches zero-day attacks that do not yet have a known signature, because the attack behaviour is abnormal even if the payload has never been seen before.

DEPLOYMENT APPROACH

Learn Mode, Then Enforce Mode — The Right Way to Deploy

One of the most common reasons organisations avoid WAF deployment is fear of blocking legitimate traffic. NetScaler WAF's two-phase deployment model eliminates that risk — you build an accurate picture of normal traffic before a single legitimate request is ever blocked. In Learn mode, the WAF observes all inbound traffic and builds a positive security model, recording which URLs exist, what parameters they accept, what content types are valid, and what normal request patterns look like; no traffic is blocked during this phase. Once the security profile is validated, Enforce mode is activated: all traffic is inspected against both the learned positive model and the OWASP signature rules, and violations are blocked at the edge, before the request reaches the application.

Phase One — Learn Mode: Build the Security Profile

- Observes all traffic without blocking any requests
- Builds a profile of valid URLs, parameters, and content types
- Identifies existing anomalies without disrupting operations
- OAS reviews learned rules and refines before enforcement
- Eliminates false positive risk before going live

Phase Two — Enforce Mode: Block in Real Time

- Blocks all requests that violate the positive security model
- Applies OWASP Top 10 signature rules in real time
- Legitimate traffic passes through without disruption
- Violations are logged with full request detail
- OAS monitors and tunes rules as applications evolve

BOT MANAGEMENT

Not All Bots Are Equal — Know the Difference

A significant proportion of web traffic is generated by automated tools — some legitimate (search engine crawlers, uptime monitors), others malicious (credential stuffers, scrapers, DDoS amplifiers). NetScaler WAF's bot management capability classifies every inbound session and applies appropriate policy to each category.

Good Bot Whitelisting

Known good bots — search engine crawlers from Google, Bing, and others, uptime monitoring services, and authorised partners — are identified by signature and allowed through without challenge. Whitelisting ensures SEO and legitimate automation are never disrupted by WAF policy.

SEARCH ENGINES & MONITORS

Device & TLS Fingerprinting

Malicious bots often fake browser user-agent strings to impersonate legitimate traffic. NetScaler WAF uses device fingerprinting and TLS fingerprinting to verify that claimed browser behaviour matches actual client characteristics, exposing bots that present themselves as Chrome or Firefox but behave like automated scripts.

BOT IMPERSONATION DETECTION

IP Reputation & Rate Analysis

Known malicious IP addresses and hosting ranges associated with botnets are blocked via IP reputation feeds. Rate analysis detects request volumes inconsistent with human behaviour, flagging sessions that generate hundreds of requests per second or attack patterns distributed across many source IPs.

REPUTATION FEEDS & RATE CONTROL

CAPTCHA Challenges

Suspicious sessions that cannot be conclusively classified are challenged with a CAPTCHA. Human users complete the challenge and proceed without disruption. Automated bots fail the challenge and are blocked. This allows NetScaler WAF to handle ambiguous traffic without either blocking legitimate users or allowing unverified bots.

HUMAN VERIFICATION

Malicious Bot Blocking & Tarpit

Confirmed malicious bots are either blocked outright or placed in a tarpit — a response delay mechanism that consumes the bot's connection resources without returning useful data. Tarpitting slows credential stuffing campaigns dramatically, making automated attacks economically impractical for attackers without exposing your systems.

BLOCK & TARPIT

Bot Traffic Analytics

Every bot interaction is logged and categorised, giving OAS and your security team full visibility into bot traffic volume, source geography, attack type distribution, and block rates over time. This data informs ongoing policy tuning and provides evidence for incident reporting and compliance purposes.

VISIBILITY & REPORTING

HOW IT'S DELIVERED

Delivered as a Managed Service by OAS

Enabling WAF is only the beginning. The real value is in correct configuration, ongoing tuning, and expert management, ensuring protection stays tight as your applications evolve and new threats emerge.

EXPERT DEPLOYMENT

Activation & Profile Configuration

OAS enables WAF on your NetScaler licence, configures protection profiles for each web application, and manages the Learn-to-Enforce transition, ensuring all policies are correctly applied before any traffic is blocked.

ALWAYS ON

Monitoring & Alert Management

OAS monitors WAF logs continuously, reviewing alert volumes, identifying attack campaigns in progress, and escalating significant incidents. You receive meaningful notifications, not raw log noise.

ONGOING TUNING

Rule Tuning & False Positive Management

As your applications change or WAF rules generate false positives against legitimate traffic, OAS adjusts policies to maintain accurate protection without disrupting users, keeping the WAF both effective and transparent.

POPIA READY

Reporting & Compliance Evidence

Regular WAF reports covering attack volume, blocked categories, bot traffic breakdown, and policy compliance, providing the documentation required for POPIA accountability, cyber insurance, and security audit requirements.

THE CITRIX SOLUTION SERIES

Citrix provides a comprehensive, secure, and high-performance digital workspace solution for any industry by centralising application and desktop management. It enables remote work, improves productivity, and strengthens security using Zero Trust principles across hybrid or multi-cloud environments. NetScaler WAF is the security layer that protects the front door, ensuring that only legitimate, safe traffic reaches your applications and users.

Citrix DaaS | Secure Private Access | NetScaler ADC | Citrix Overview

Ready to Activate WAF Protection on Your NetScaler?

Speak to an OAS consultant about enabling and managing NetScaler WAF for your web-facing applications, using the licence you may already own.

TELEPHONE

+27 11 485 3454

EMAIL

info@oas.co.za

WEB

https://www.oas.co.za

OFFICE

25 Durham Street, Raedene Estate, Johannesburg

Request a demo: https://www.oas.co.za/contact/demo

Open Architecture Systems — Protect. Detect. Recover. Citrix Platinum Partner since 1987.