Cyberoam
A SOPHOS Company

NG Future-ready

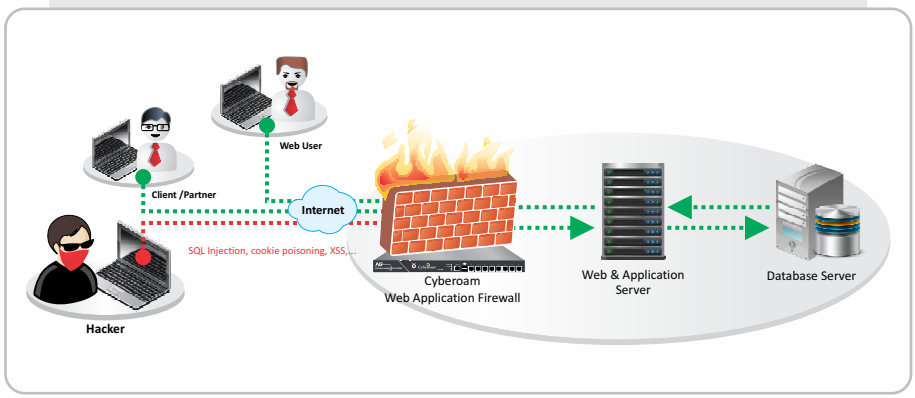
Web Application Firewall Subscription on Cyberoam Network Security Appliances (UTM, NGFW)

Tech Sheet

With critical legacy applications like CRM, ERP, inventory management, banking, and more, moving to the web, hackers are increasingly targeting vulnerabilities present in such web-applications to break into organizations' IT networks. Organizations need a WAF to keep their web applications secure.

Cyberoam offers comprehensive network security, which includes protection of WAF, for physical as well as virtualized environments. Cyberoam's WAF feature, available as a subscription module for Cyberoam's hardware and virtual network security appliances#, follows the positive security model to secure websites and web-based applications against attacks like SQL injection, cross-site scripting (XSS), URL parameter tampering, and more, including the OWASP Top 10 Web application vulnerabilities.

Cyberoam Web Application Firewall Protection against Web-based Application Attacks



Cyberoam WAF is deployed to intercept the traffic to and from the web servers to provide an additional layer of security against attacks before they reach the web applications. Cyberoam WAF's Intuitive Website Flow Detector intelligently "self-learns" the legitimate behavior and response of the web applications and ensures the sanctity of web applications in response to server requests, protecting them against web application attacks. Cyberoam WAF looks at every request and response within the HTTP/HTTPS/Web Service layers. It is effective at repelling attacks from a wide range of commercial and open-source automated vulnerability scanners (e.g. Nessus, WebInspect), as well as hand-crafted attacks.

Cyberoam WAF Features

Positive protection model without Signature Tables
The Cyberoam WAF enforces a positive security model through Intuitive Website Flow Detector to automatically identify and block all application-layer attacks without relying on signature tables or pattern-matching techniques.

Comprehensive business logic protection
The Cyberoam WAF protects against attacks like SQL injection, cross-site scripting (XSS), and cookie-poisoning that seek to exploit business logic behind Web applications, ensuring they are used exactly as intended.

HTTPS (SSL) encryption Offloading
Attackers cannot bypass the Cyberoam WAF protection measures through an HTTPS (SSL) connection, mostly used in organizations that process sensitive data. The WAF not only secures encrypted connections, but also reduces latency of SSL traffic with its SSL offloading capabilities.

Instant Web server hardening
The Cyberoam WAF instantly shields any Web environment (IIS, Apache, WebSphere®, etc.) against common server mis-configurations and an ever-expanding universe of known 3rd-party software vulnerabilities.

Reverse proxy for incoming HTTP/HTTPS traffic
The Cyberoam WAF follows a reverse proxy model for all incoming HTTP and HTTPS traffic which provides an additional level of security by virtualizing the application infrastructure. WAF receives all incoming connections from the Web client and then refers to the server in order to fulfill those requests. The client never gains direct contact with the server thus hiding the existence and characteristics of originating servers.

URL , Cookie, and Form hardening
Cyberoam WAF protects Application-defined URL query string parameters, cookies, and HTML form field values. It automatically identifies and blocks attempts to escalate user privileges through cookie-poisoning, gain access to other accounts through URL query string parameter tampering, and other types of browser data manipulation.

Monitoring and reporting
Cyberoam WAF provides alerts and logs that help organizations with information on types of attacks, source of attacks, action taken on them, and more that help comply with the PCI DSS requirements.

Additional Features:
- Block/alert known bad IP addresses
- Customizable user messages for blocked requests
- Rate-based connection safeguards

#For Performance figures of Cyberoam virtual Network Security Appliances, refer to the Cyberoam virtual Security techsheet.

Cyberoam WAF Feature Specifications

Web Application Security
- Brute Force Attacks Mitigation
- Cookie Protections Measures
- Session Attacks Mitigation
- Cryptographic URL and Parameter Protection
- Strict Request Flow Enforcement
- HTTPS (SSL) encryption offloading
- HTTP-based worm/virus protection
- Banner-grabbing protection
- Hidden field manipulation protection
- SQL injection protection
- OS command injection protection
- Cross-site scripting protection (XSS)
- Dangling pointer protection
- Stealth commanding protection
- Buffer overrun protection
- URL Hardening engine
- Form field meta data validation
- Directory traversal prevention
- Response control
  - Block client
  - Reset connection
  - Redirect
  - Custom response
- Outbound data theft protection
  - Credit card numbers
  - Social Security numbers
  - Custom pattern matching (regex)
- Protocol limit checks
- File upload control

Protocol Support
- HTTP/S 0.9/1.0/1.1

Management
- Web-based configuration wizard
- Role-based Access control
- Firmware Upgrades viaWebUI
- Cyberoam Central Console (Optional)
- NTP Support
- Web 2.0 compliant UI (HTTPS)
- UI Color Styler
- Commandline interface (Serial, SSH, Telnet)
- SNMP(v1, v2)
- Multi-lingual support: English, Chinese, Hindi, French, Japanese

Reporting
- Real-time network, HTTP alerts
- Detailed activity log
- Web notification
- Full transaction log of all activity in human-readable format
- System log
- Web Firewall log
- Access log
- Audit log

Compliance
- CE
- FCC

Specifications	Backend servers supported	HTTP requests per second	WAF Protected Throughput (Mbps)
Cyberoam NG series			
CR 25iNG	5	400	100
CR 35iNG	10	800	150
CR 50iNG	15	1,200	450
CR 100iNG	20	1,500	700
CR 200iNG/XP	25	2,000	1,000
CR 300iNG/XP	30	2,500	1,250
CR 500iNG-XP	50	3,200	1,500
CR 750iNG-XP	80	4,000	1,750
CR1000iNG-XP	125	4,800	2,000
CR 1500iNG-XP	200	5,500	2,300
CR 2500iNG-XP	300	6,500	2,600

Specifications	Backend servers supported	HTTP requests per second	WAF Protected Throughput (Mbps)
Cyberoam Virtual Network Security Appliances			
CRiV-1C	5	500	300
CRiV-2C	10	700	500
CRiV-4C	25	1,000	800
CRiV-8C	40	1,400	1,400
CRiV-12C	50	1,550	1,550

*Not available in case of bridge pair configurations

Toll Free Numbers
USA : +1-800-686-2360 | **India :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958