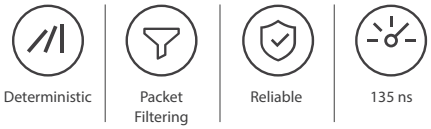
MetaProtect™ Firewall

Latency-optimised packet filtering in as low as 135 nanoseconds



MetaProtect Firewall is a network application that runs on the 7130L Series devices performing line-rate low-latency parallel packet filtering and logging between port-pairs.

Filtering is implemented via per-port Access Control Lists (ACL). MetaProtect Firewall provides complete flexibility in configuration, allowing authenticated administrators to create mappings between physical port-pairs and apply either uni or bidirectional security policy.

MetaProtect is ideally suited for deployments where compliance legislation mandates the use of a Firewall, but where the lowest possible latency is critical to business viability. With both packet inspection & forwarding occurring in as little as 135 nanoseconds; MetaProtect offers a significantly faster solution than traditional firewalls.

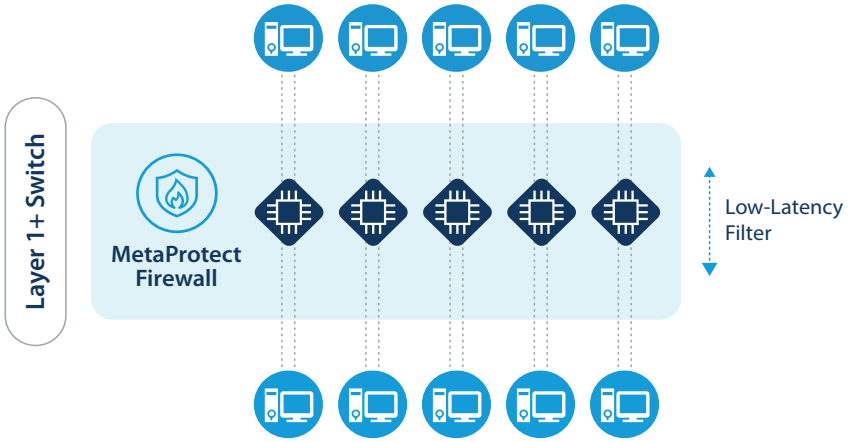
Administrators may also define port-pairs, or directions, that do not require filtering, in which case packets are passed through in 5 nanoseconds. Any ingress port, pre or post ACL, may be configured to fan out to multiple egress ports allowing for maximum flexibility based upon the desired filtering architecture.

In addition to being discarded, any packets not conforming to the defined security policy are logged. Logging involves the collection & exporting of the entire packet header, ensuring MetaProtect meets even the most stringent compliance requirements.

FEATURES	BENEFITS
Parallel filtering	Cut-through filtering via 32 ACLs with up to 510 rules per ACL. Per-port filtering possible by assigning an ACL to a port.
Flexible ACLs	ACLs support permit/deny rules based upon source/destination MAC/IP address/Port number. IP addresses may be wild-carded using CIDR style notation.
Ultra-low latency filtering	Average filter latency of 135 ns for the minimum latency configuration (1 rule) to 161 ns for the maximum configuration (510 rules).
High port density	48 x 10GbE SFP+ ports in 1 RU with 32 x 10GbE Firewall filters and accelerated traffic processing capacity.
Extensive packet statistics	Advanced monitoring and capture of comprehensive packet statistics across all ports. Support for detailed switch statistics via SNMP, CLI or InfluxDB.
Comprehensive logging	• Logged statistics of permitted and denied packets • Individually logged events when packet fails an ACL, including packet information, date, time, ACL ID and reason • Logged administrative ACL rule changes • Local and remote logging via syslog.
Easy to monitor and manage	Advanced monitorArista provides a complete range of additional features including: • A comprehensive set of Ethernet counters on each port • An integrated Linux management processor • Streaming telemetry to a remote InfluxDB database • Command-line interface (CLI) via secure shell (SSH), Telnet, serial connection • Local and remote logging via Syslog • JSON-RPC API • Simple network management protocol (SNMP) v1, v2, v3

Optimized for

- Arista 7130L Series with embedded Xilinx Ultrascale/Ultrascale+ FPGA(s).



Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062