NSE7000 Security Services Load Balancer

NSE7200 (10G License)

32 x 1/10G SFP+

230 Gbps Throughput

312 Mpps Forwarding Rate

Upgradable to 100G with software license

NSE7200 (100G License)

2 x 100G QSFP28
32 x 1/10G SFP+

230 Gbps Throughput

312 Mpps Forwarding Rate

Security Services Load Balancer Designed for the Virtualized World

NSE7000 ("NSE") is a security service load balancer that enables organizations to scale out their network security appliances, and provides an easy path to virtualizing network security.

NSE's high performance processing engine classifies and redirects traffic into load balanced service chains based on user defined, programmable rules. In addition, within the same traffic processing engine, the NSE lets you enforce security policy based on any real-time security analytics.

NSE offers:

- Truly transparent bump in the wire operation
- High performance traffic processing engine
- Support for virtual and physical appliances in service chains
- Symmetric, bi-directional load-balancing of in-line devices within service chains
- Automatic failure detection and bypass of the service chain
- Built-in high fidelity IPFIX probe
- REST programmability

Scale Your Security

Processing larger and larger volumes of traffic can no longer be done in a single security appliance. The majority of network traffic today is encrypted and traditional security appliances lose over 90% of their rated throughput when handling encrypted traffic. Truly scalable network security architectures require scaling out security appliances to provide inspection of all traffic.

By load balancing security appliances in virtual wire mode, the NSE allows traffic inspection at any throughput while dramatically reducing the complexity of deployment and operation. The NSE supports both physical and virtual security appliances, enabling organizations to maximize their existing investments into hardware appliances, and providing them a smooth migration path to virtualized network security.

Security Service Chaining Made Simple

NSE is deployed in a fully transparent virtual wire mode with default accept policy so no changes to routing or switching are required. From there, the NSE gives you full control of the traffic through a simple REST API interface that programs all of its functions, including provisioning, monitoring, and rule management.
Build up to 64 virtual wire service chains, and selectively redirect the traffic into them using classification rules. Each service chain can have up to 128 members, and the traffic is automatically load balanced symmetrically in both directions.

Support for both physical and virtual appliances in service chains and NSE's ability to load balance between them allow you to build security infrastructure that scales elastically with your evolving traffic needs. Advanced path checks and real-time statistics ensure the highest availability of your security inspection service chains.

Use your automation and DevOps tools to provision and manage the NSE and virtualized security infrastructure, and now your network security looks just like a private cloud application.

Then Make it Cloud

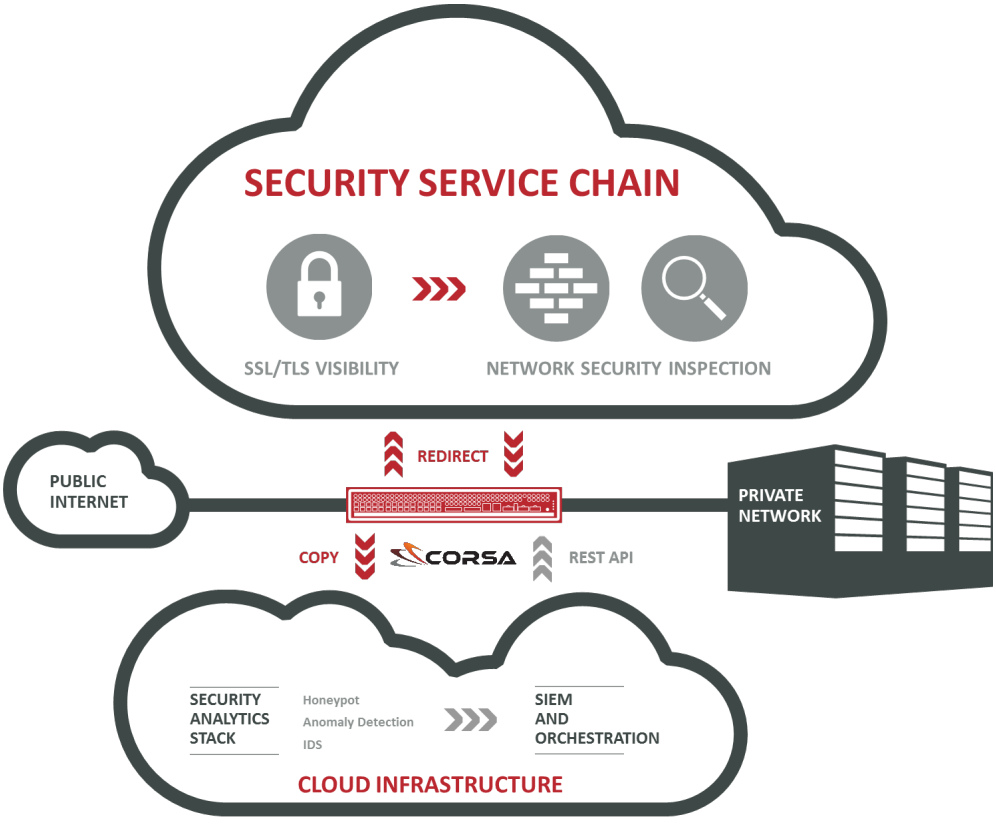
Once you have the NSE giving you scale for 100% traffic inspection, you can further evolve and optimize your security. NSE can feed security analytics tools with both copies of actual traffic and high fidelity IPFIX information.

Analytics do not need be done on premise. These applications are well suited to cloud-based deployments and can provide:

- Network and security performance monitoring
- Anomaly detection
- Dynamic deception
- Behavior analytics

Using the results of the analysis from cloud based analytics tools, the NSE can easily block or rate-limit traffic in the network independently from where the detection and analytics are performed. This high performance enforcement point further offloads in-line security inspection.

Corsa NSE solution gives you software defined network security by delivering: service chaining, scale out of physical or virtual appliances and high performance enforcement.



How NSE Works

NSE is deployed as a transparent virtual wire device. For each virtual wire one or more service chains, or alternate paths, can be defined. Each alternate path can have up to 128 members, which are a physical port or a logical subinterface representing a virtual appliance. NSE's Traffic Processing Engine classifies and redirects the traffic into the service chains.

Load Balancing

There can be up to 64 service chains configured on the system. The NSE's Load Balancing Engine automatically load balances the traffic between all members of the service chain.

Each member can have a weight configured for them, and the traffic will be distributed accordingly. In addition, the NSE ensures that both directions of the same TCP or UDP connection are always sent to the same in-line appliance and this is always guaranteed.

Built-in Path Checks

NSE has an automatic path check mechanism that monitors if a member of the service chain is operational. When a failure is detected, the traffic is no longer sent to that member, and is redistributed between all other operational members.

A configuration policy can specify whether the wire fails open or fails closed when all members are down. Additionally the path check mechanism can detect incorrect wiring or connections for both physical and logical topologies.

Traffic Classification

Traffic on any virtual wire that is configured on the NSE is always processed by the NSE Traffic Processing Engine. This is done in hardware based on full Layer 3 and Layer 4 information.

Filter keys for classification rules include: GigaFilter™ ACL member, destination IP, source IP, port, destination port, source port, ICMP type, ICMP code, IPv4 protocol, IPv4 DSCP, IPv6 next-header, and IPv6 traffic class.

Classification rules also have action associated with them.

Classification Rule Actions

- Accept — Traffic will follow the default path. Default action type.
- Discard — Traffic is dropped.
- Redirect — Traffic is redirected into a service chain.
- Traffic-rate — Traffic is rate-limited to the specified rate, and put on the default path.
- Traffic-marking — Traffic has DSCP field remarked.

Default redirect can also be configured on any virtual wire, where all traffic on that wire is redirected into a service chain.

GigaFilter™ ACL

Hundreds of thousands of classification rules not enough to identify all IoCs? Use a separate IP ACL that can accept every possible IPv4 address. 4,294,967,296 addresses in a single ACL. No more scale problem for filtering botnets or other threats.

Packet Replication

Intelligently copy packets to out-of-line IDS or forensic inspection devices based on specific copy rules. Copy rules can match on IPv4 and IPv6 Layer 3 and Layer 4 information, and are programmed independently from the classification rules via REST API. Optionally, packets can be sampled and/or truncated.

Built-in High Performance IPFIX Exporter

The NSE exports high fidelity IPFIX flow records for the ingress traffic of all wires. Flow records contain all relevant IPv4 and IPv6 information as well as GigaFilter membership metadata. The Corsa NSE is optimized to produce unsampled IPFIX data for the full forwarding rate of the platform.

Packet Rate	312 Million packets/second
Sampling Rate	Up to 100% or 1:1
Cache Size	4 Million flows
Flow Export Rate	Up to 1 Million flows/second
Export Latency	<1 second
Active Timeout Range	1-60 seconds
Idle Timeout Range	1-60 seconds

Platform Specifications

High Performance Security Services Load Balancer	
Throughput	230 Gbps
Forwarding Rate	312 Mpps
Packet Buffer Memory	6 GB
Number of Virtual Wires	16
IPFIX Probe	Up to 1:1 sampling, 4M flow cache, 1M flows/sec export rate
Real-time Traffic Statistics	Packet and Byte Counters Per Rule
IPv6 Support	Yes
Classification and Service Chaining	
Packet Classification and Matching	Layer 3 and Layer 4 Header Fields
Per Rule Actions	Redirect, Accept, Discard, Rate-Limit, DSCP Remark
Number of IPv4 5-tuple Rules	220,000
Number of IPv6 5-tuple Rules	60,000
Number of Service Chains	64
Number of Load Balanced Members in Service Chain	128
Rule Update Rate (BGP Flow Spec)	~2,500 updates/sec
GigaFilter™ ACL	4,294,967,296 IPv4 address entries
Packet Replication	
Packet Classification and Matching	Layer 3 and Layer 4 Header Fields
Number of Copy Rules	1000 (IPv4) and 16 (IPv6)
Number of Copy Profiles	15
IPv6 Support	Yes
Management	
Management Interface	10/100/1000Base-T RJ-45 (Out-of-band)
Device Configuration and Management	REST API, CLI
Enforcement Rule Management	BGP Flow Spec (RFC 5575), REST API, CLI
Enforcement Rule Statistics	REST API, CLI
Copy Rule Management	REST API, CLI
Physical	
Chassis Rack Height	1 RU, 19” Rack mount
Typical Power	450W
Ports	2 x 100G QSFP28, 32 x 10G/1G SFP+
Power Supplies	2 x AC or 2 x DC Redundant
Ventilation	Front-to-back or back-to-front
Regulatory Compliance	FCC, CE, NRTL, RoHS, WEEE, IEC, CSA, RCM

Corsa Technology reserves the right to modify or remove product specifications without prior notice.
For more information contact us at sales@corsa.com.