CORSA

TECHNICAL OVERVIEW

What Makes Corsa NSE7000 So Great?:

A Technical Overview of the Security Services Load Balancer

Summary

The Corsa NSE7000 security services load balancer is at the heart of an automated and virtualized network security strategy, offering highly programmable on-demand security perimeters and per tenant security policy applied at your gateway.

We stepped back to rethink network security architectures and define what is needed to add the missing virtualization and automation. We have innovated with a highly programmable at-scale network security appliance. We enable you to add and automate security services at network speed without having to change your network architecture or sacrifice performance.

Keep your software investments, develop machine learning, build in artificial intelligence – and let the Corsa NSE7000 appliance virtualize your network security and protect your network against escalating cyber threats.

Contents

Introduction

The Corsa NSE7000 appliance is an L2 transparent, in-line security services load balancer with high precision flow forwarding via user defined, programmable rules. Super easy to deploy and use, it is a flexible appliance to scale and automate network security.

In conjunction with existing threat detection, security information and event management (SIEM), artificial intelligence and analysis tools, the NSE7000 appliance can take on any number of roles in the network. Unlike single function middle boxes, the NSE7000 security services load balancer can be used for dynamic security service chaining, on-demand security perimeters, or automated per tenant security policy enforcement. Insert the NSE7000 appliance anywhere in any sized network to instantly add at-scale, virtualized network security where you need it. Gone are the days of a fixed security perimeter.

Change the Way Network Security is Done

Virtualizing network security is taking hold. This evolution doesn't obviate the need for firewall, intrusion detection systems (IDS)/intrusion prevention systems (IPS), and gateway functions, but it does mean that delivering these functions in fixed appliances is old school and security and network architects are moving away from specialty boxes.

And what are they doing instead? They are spinning up virtual instances of those functions, they are putting all the intelligence in software – SaaS is a great model. And they are looking for user programmable load balancing on the wire to direct traffic at any scale to these virtual functions and services.

This is where Corsa comes in. We are a fundamental element in this wave of change. Corsa simply and consistently moves traffic, always line-rate, at any speed and any scale, without network compromise, to the right services and functions, virtualized wherever and whenever required. This means you can scale your traffic visibility to 100%, even when traffic is encrypted.

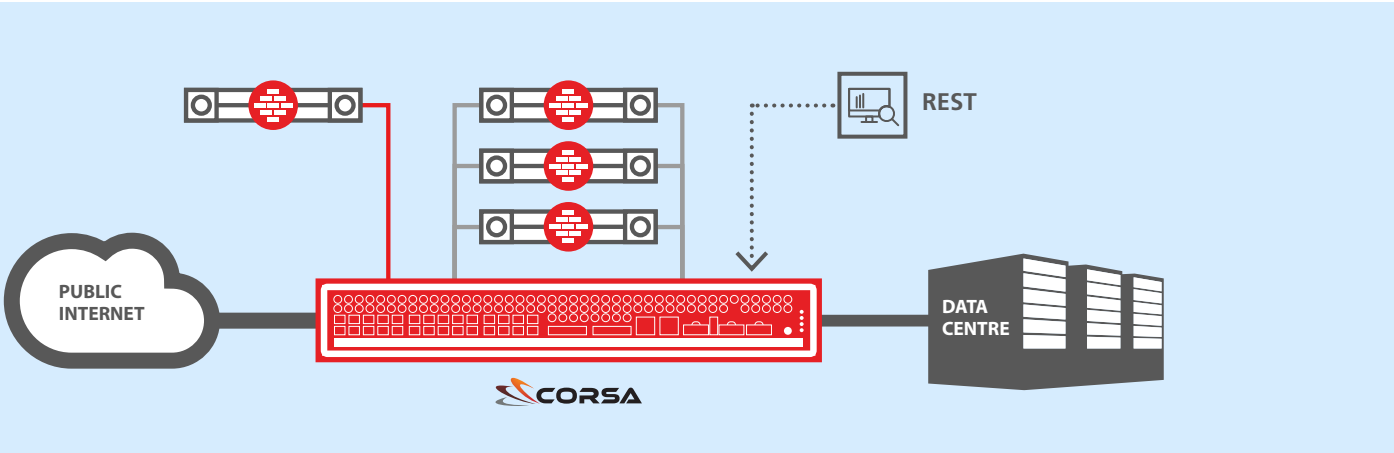
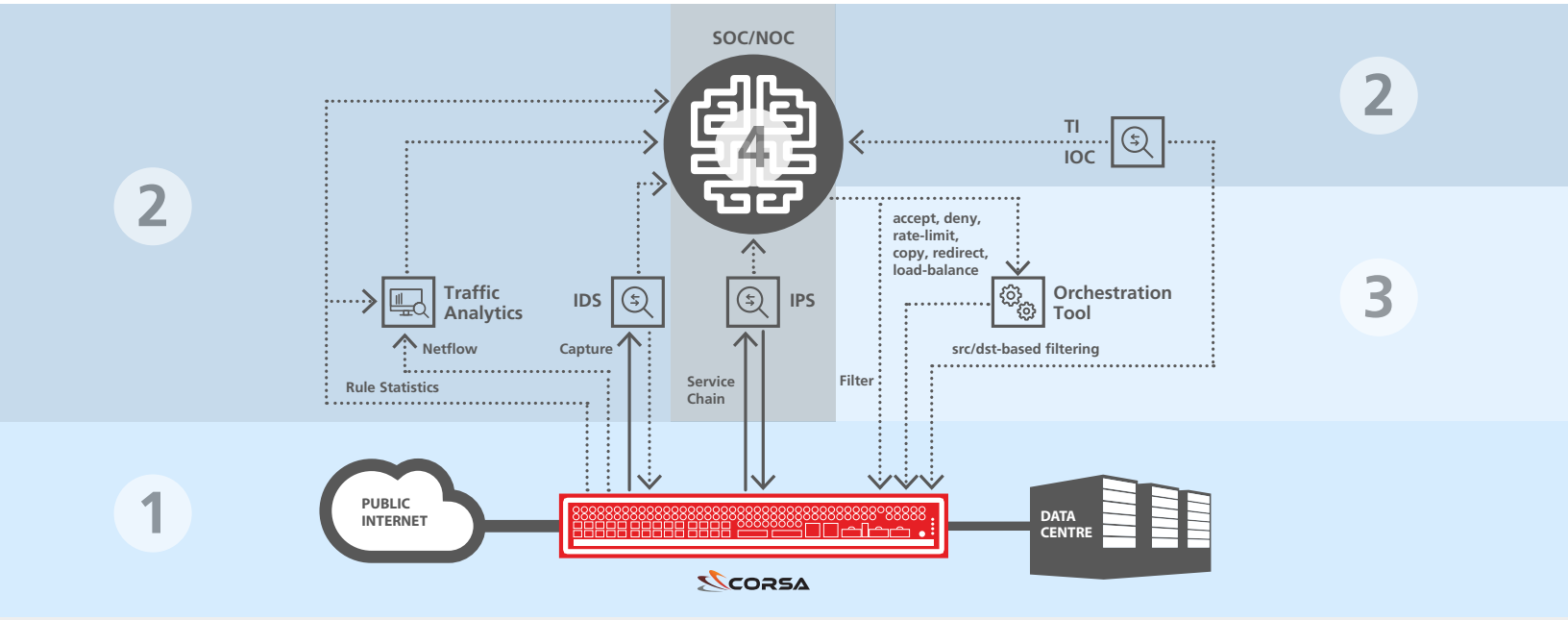


Figure 1: Dynamic Programmable Control for Filtering Traffic

What Does Corsa NSE7000 do for You?

Take any link in your network, in-line on that link you can place a Corsa NSE7000 security services load balancer. It's L2 transparent to the network so you don't touch your existing network configuration, you don't add network complexity nor new attack surfaces. It's designed to operate within any software ecosystem so you don't need to modify your existing SecOps environment. With full line-rate performance, the NSE7000 appliance lets you load balance traffic into any number of virtual or physical security functions. So you can start by scaling your existing physical appliances and then move to full virtualization over time.

You can also create a control point to act as a traffic export for data acquisition and statistics while simultaneously using it as an enforcement point for traffic filtering to maintain integrity of the network. So any number of flows can be manipulated using any rule with a wide choice of actions: accept, drop, rate-limit, copy, redirect, GigaFilter™ ACL and more. The NSE7000 appliance gives you dynamic and programmatic traffic forwarding without the need to re-architect your network.



1 LOAD BALANCER

The NSE7000 appliance is a security services load balancer that offers extreme scale for service chaining with the option to do enforcement. It's an all in one product that can be placed anywhere in the network and interface with any security software. For those needing to scale SSL/TLS visibility, the NSE7000 appliance is ideal for spreading traffic to multiple SSL/TLS decryption/encryption products.

2 IDS

The NSE7000 product copies traffic at any operator-defined granularity to select very precise flows for inspection. When anomalies are flagged, the NSE7000 appliance can be part of a 2-step approach to enforcement that involves using it to rate limit upon initial detection of suspicious traffic. This buys time for the alarm to be investigated and escalated to the right level while protecting network integrity. Then your second step involves the specific enforcement action required, whether drop or allow (or continue to rate limit).

3 NEXT-GENERATION FIREWALL

Use the NSE7000 GigaFilter as a simple, single in-line control to blacklist millions of bad IP addresses and let your routers' ACLs do the routing. Automatic, instant gateway protection with support for 4B+ IPv4 addresses and 10s of millions of IPv6.

4 IPS

For security function chaining, use the NSE7000 appliance to skim (we also call it redirect) traffic to your IPS for inspection. So you can have whatever NGFW or web application firewall or any other security function hanging off the NSE7000 appliance, virtually or as an appliance, and you can spin up more services dynamically as you need them.

3 ENFORCEMENT

You have the intelligence, now you need to automate the action. Use the NSE7000 appliance to dynamically enforce your security policy by filtering out unwanted traffic to maintain network integrity. You can allow, block, rate-limit or redirect flows with as much granularity as you need, from the isolated flow to whole subnets.

2 TRAFFIC ANALYTICS

You want all the data you could possibly get at times and at other times you want something very specific. With the NSE7000 appliance, you can extract any amount of traffic from a single flow to wholesale copies of traffic and export it to any analytics tool using NetFlow or by polling any number of rules statistics.

In the easiest possible way, you can create dynamic network control by placing the NSE7000 appliance in-line wherever you need it. So if you need to create a scalable security perimeter, add the NSE7000 appliance as an enforcement point. Want to scale your firewall? Then redirect traffic to virtual firewall instances that dynamically expand and contract your gateway protection. Or perhaps you are leading the incident response team and need to buy time for further investigation, then rate-limit certain traffic to maintain network integrity while you dig deeper. If you are a managed DDoS service and you want to clear out DDoS traffic, then control traffic flow based on whatever filters you need at the time and rapidly adjust them to some new customized filter based on your intimate and proprietary knowledge of good traffic vs attack traffic. If you are protecting your enterprise and want to isolate a critical department, then control based on user or traffic type and policy.

How Does it Work?

RAW PERFORMANCE

Easily automated and blazing fast, the NSE7000 hardware is a thoughtfully architected combination of merchant silicon and FPGAs. So much more than a chip in a box, and definitely not just an array of x86 CPUs stuck together hoping for speed, the platform is hyper optimized for high speed, maximum programmability and ultimate user control.

We took the concept of an FPGA-based traffic processor and built out from there. The NSE7000 appliance has dedicated hardware parts for all of its most important functions, including ultra-fast GDDR5 memory for packet buffering, special SRAM for keeping track of every possible statistic in real time, general purpose DDR3 RAM for off-chip memory offload, hardware based algorithmic search engines for large scale super-fast TCAM-like searches, and last but not least, best in class ASIC based switching fabric found in the most high performance routers available today. In addition to all that data-path hardware, you also get a powerful server-grade management module with an Intel Core i7 processor running a full Linux server based OS.

All this was designed in an innovative way, with Corsa ingenuity applied to figure out how to build the fastest, most flexible network security services load balancer out there. The result: an appliance that scales network security like nothing else on the market. You get to decide what you want to do with traffic at each and every control point in your network. This means you can add network security wherever you need it and have fully automated control over what happens.

OPERATOR-DEFINED PROGRAMMABLE RULES

The NSE7000 appliance gives users complete control over their traffic. Whether you call it flow-based networking, or fine grained traffic control, the point is that you can write your own rules that can match traffic on every L3 and L4 header field, and then act on each packet accordingly. All in real time.

Our hardware based enforcement engine busts open each and every packet header as the packets are forwarded, and if the packet matches any rule in the enforcement engine, the hardware executes the action. Not only can you accept and deny matching traffic, you can just as easily rate-limit, remark DSCP or redirect matching traffic from the default path to a parallel path with an in-line inspection device.

If you are more comfortable with REST, we give you an extremely simple JSON based REST API to manage all the rules, or for network veterans, you can use BGP Flow Spec to accomplish the same thing.

Last, but not least, you have access to hundreds of thousands of rules in the enforcement engine with no impact to the device performance. Our hardware is built in such a way that our forwarding rate as well as latency through the box are always constant.

UNCOMPROMISED NETWORK SPEED AND SCALE

Traffic throughput and packet processing is guaranteed to be line-rate regardless of what the NSE7000 appliance is having do in terms of steering traffic to service chains, or blocking an IoT-sourced DDoS attack, or rate-limiting discrete suspicious flows.

10G, 100G or even more traffic doesn't matter to the NSE7000 appliance because of our innovative hardware design that guarantees a constant packet processing rate regardless of the number of rules programmed. So you cannot overwhelm the NSE7000 appliance. No traffic pattern, no throughput and no amount of policy or rules will cause it to slow down or unexpectedly drop packets. Check out our performance report to appreciate this further.

AUTOMATIC FOR THE PEOPLE

Just like our hardware was built with a completely new approach to managing traffic, we built the control interface for our platform to be future forward. We didn't bolt on some heavy interface on top of a 10 year old operating system that was designed before all your automation existed. We built a modern REST based interface right into the platform, which gives you full control of all the functions of the hardware through a simple human readable JSON based API. Our own CLI is built on top of the same interface, so you know that you have as much control through the CLI as you have through REST.

For rules management in addition to REST you also get a BGP listener that understands Flow Spec (RFC5575). That way if you prefer BGP Flow Spec as your rule management protocol, you can use it with your existing tools.

All this allows you to integrate the NSE platform into your automation tools or any other security product that needs to act on network traffic in immediate response to an alert. In conjunction with our raw packet processing performance, and complete network transparency, this gives you the path to get your machine learning and AI security systems to react to security events within the network in real time, without being afraid that a new automatic rule takes out the whole device.

With a newfound ability to implement at the speed of change, your aptitude for effortlessly affecting zero-day service updates relevant to your requirements will ensure everyone will be seriously impressed with how quickly and easily new services are actualized.

On-demand security perimeters with dynamic provisioning are just a click away. Need automated DDoS protection? Trying to deploy a more simplified virtualized network security architecture? Having troubles keeping up with changing threats? The NSE7000 appliance enables virtualized service delivery that optimizes your operations and will delight your customers with how quickly and easily new services are stood up.

UNPRECEDENTED INSIGHTS

The NSE7000 appliance gives you extreme visibility into your traffic with separate statistics counters for bytes and packets, logging the details for every rule hit at every single packet decision point within the device. These stats are maintained in dedicated hardware, and are read by the OS in sub-second intervals. This is a dramatic improvement from traditional network security devices that aggregate multiple stats into one counter, don't give you enough visibility into what is going on, and have long polling intervals.

Furthermore, the NSE7000 appliance has a built in NetFlow/IPFIX probe that lets you see what traffic is passing through the wire without having to sample the flows. The probe sits before the enforcement rules engine, so you get the NetFlow statistics of the raw input before any of the rules are applied.

GIGAFILTER ACL

Another innovative feature that makes NSE7000 truly unique is our patented GigaFilter ACL, a source-address ACL that can hold 4,294,967,296 entries which is every possible IPv4 address. You can use this to fight large botnets with tens of millions of members in the near future. Or you may want to use all the IOC/TI feeds that you have at the same time, without having to triage the entries.

You can use GigaFilter in conjunction with all the other rules and actions in the enforcement engine to create a sophisticated first line of response to your network security.

For example, if you don't want to just blindly blackhole all traffic from all sources, but rather only want to drop attack traffic to a specific victim on UDP port 53, just add a rule like this:

```
POST
https://nse.example.com/app/rules/vsc1/v1/sources/rest/rules
{
"rule": 1,
"afi": "ipv4",
"filters": {"dst-ip": ["192.0.2.1"],"gigafilter: ["present"],"proto": ["=udp"],
"dst-port":["=53"]},
"actions": [{"action-type": "discard"}]
}
```

And it will drop matching traffic for all sources in the GigaFilter, whether there are 2 in there, or 200 million. It's that easy.

About Corsa

Corsa Security is leading the transformation of network security with a private cloud approach that helps large enterprises and service providers scale network security services with unwavering performance, unparalleled flexibility and unmatched simplicity. By leveraging unique networking expertise and proven virtualization technologies, Corsa Red Armor is a turnkey network security virtualization platform that you order with one click, deploy in minutes and pay-as-you-grow to scale traffic inspection for 100% visibility and better ROI compared to existing approaches.

To start on your software-defined network security journey, visit corsa.com.

Please contact us

For more information about Corsa solutions please contact us today.

11 Hines Rd. Suite 203
Ottawa, ON Canada K2K 2X1
613 287 0393

sales@corsa.com
www.corsa.com