Data Sheet

Indigo Software-Defined Firewall

Flexible, carrier-grade security for communications service providers

The Indigo Advantage

- Achieves full visibility into network traffic at line speed with state-of-the-art DPI engine
- Secures and control messaging, VoIP and other applications over mobile, fixed telecom, satellite and public IP networks
- Controls prohibited traffic without hindering access to key communications and Internet services
- Increases network operator revenue by minimizing false positives
- Regular application and protocol updates eliminate need to for custom development and maintenance
- Fast and easy to deploy

Overview

When it comes to monitoring and securing communications services, SOC teams need solutions that meet their unique challenges. Designed specifically for the requiremets of CSPs, the Indigo Software-Defined Firewall (SDF) delivers carrier-grade performance and availability. It is currently in-line at large-scale deployments such as monitoring and controlling traffic at national telecom companies or securing the entire Internet infrastructure of a country.

The Indigo Software-Defined Firewall (SDF) is a multi-vendor solution designed specifically for network operator Security Teams that need a customized, personalized Firewall / DPI solution to address today’s complex security and compliance concerns. It combines next-generation firewall features with a software-defined architecture to simplify complex security management. The industry’s highest-performing DPI engine provides near-real-time visibility into network traffic.

Plus, it gives mobile, fixed telecom, satellite data and ISP SOC teams the flexibility to establish policies for controlling applications and user access to URLs using a modern scripting language. An Elastic Stack integration, which includes the Kibana dashboard, further simplifies management and speeds incident response time.

Next-Generation Firewall for Large-scale Networks

With the growth of IP-enabled communications, encrypted applications and user demands for unfettered access to key services, network operators face enormous compliance challenges. They must also provide carrier-class reliability, which is vulnerable to DDoS attacks, application layer intrusions, APTs and malware, and other threats. At the same time, they most assure the availability of customers' hosted services and protect their data.

The Indigo SDF provides integrated next-generation security along with centralized management. WAF capabilities also defend against SQL injection and other application layer attacks, while anti-DDoS protects the availability of not only your network infrastructure but also your customers' hosted services. Key capabilities include:

- Network security monitoring
- Intrusion detection
- Intrusion prevention
- Data leakage protection
- Web application protection
- DDoS protection
- Historic and real-time threat reporting

Gain Real-time Visibility with Highest-Performing DPI Engine

The Indigo SDF integrates the R&S® PACE 2 DPI engine from the German cybersecurity leader Rohde & Schwarz epoque. With throughput of up to 32 Gbps per core, it is the the highest performing DPI engine available today. The R&S PACE 2 also provides state-of-the-art IP traffic analytics capabilities, including behavior analysis. The DPI solution also performs Protocol Decoding (open protocols like HTTP, DNS, e-Mail, FTP, etc.).

Regain Control of Activity and Access

The Indigo SDF restores visibility into network traffic made opaque by encrypted applications and obfuscated or masked traffic path techniques such as domain fronting. It can also granularly control what applications are permitted, prioritized or de-prioritized for access. An advanced scripting engine allows SOC teams to flexibly and dynamically implement policies. These policies can control subscriber activity such as use of VoIP and encrypted messaging apps or access to prohibited or malicious URLs.
The SDF also enforces network access controls and regulates IP-based communications network traffic with integrated awareness of applications. This includes subscriber local IP-address visibility, which enables the implementation of subscriber-specific rules and also improves the detection of certain applications.

Scripting Engine

Indigo SDF policies are written as scripts based on the Lua programming language and provide the following features:

- **Flexibility:** Policy rules, lists and objects can be integrated with external systems. (RADIUS, SQL, HTTP, etc.) and data feeds (IP reputation database and malware hash lists); data can be arbitrarily processed (JSON, XML, CSV, etc.).
- **Just-in-time compiler:** Scripts are compiled to native x86 machine code for optimal performance.
- **Dynamic reload:** Scripts can be reloaded live in production without restarting the firewall, and all state information is retained.
- **Sandbox:** Scripts are memory-safe and sandboxed; errors in scripts cannot crash the main firewall processes.

Quickly and Cost-Effectively Comply with Regulations

The Indigo SDF is specifically designed to streamline compliance. It enables CSPs to quickly and cost-effectively comply with government mandates such as monitoring and controlling apps and access to harmful websites or blocking IP telephony (VoIP). Capabilities include:

- Data Retention
- Governing access to websites / URLs
- Governing applications traffic — including encrypted messaging
- Blocking protocols / proxies / VPNs

Network Management

Raise your network's quality and streamline your business practices with sophisticated traffic management for telecom, Wi-Fi and broadband networks. Capabilities include:

- Captive portals
- NetFlow probe
- Traffic analysis
- Shaping and optimization
- Charging and billing

Carrier-Grade Performance and Availability

The Indigo SDF is designed from the ground up as a carrier-grade security technology it provides:

High Availability

- Bypass mode – prevents network outages in case of power or hardware failure
- Hot standby – Automatic failover time of one second

Low Latency

- Zero-copy packet processing and forwarding architecture – bypasses host kernel to achieve minimal latency and maximum throughput
- One-pass architecture
- < 0.1 ms

Wire-speed Throughput

- 10G wire-speed
- 14.8M packets per second

Operation Modes

The Indigo SDF is typically installed between the BRAS and NAT elements in the network, and can be configured to run in three modes:

- **Inline mode** – Acts as transparent network bridge between two ports. This is the recommended mode.
- **Monitor mode** – Acts as network analyzer on mirror (SPAN) port.
- **Passive mode** – Analyzes network traffic on mirror (SPAN) port and injects packets (TCP reset, DNS response, HTTP redirect, and ICMP unreachable) on the side.

Hardware

The Indigo SDF is available as software only or pre-installed on a 2U rack-mounted Indigo network appliance in 1Gbps and 10Gbps models.

Available Models

	SDF1G	SDF10G
Form Factor	2U	2U
CPU	2 x Quad-Core Intel® Xeon® processor E5-2609 v2 2.50GHz 10MB Cache	2 x 18 Core Intel® Xeon® processor E5-2697 v4 2.30 GHz 45M Cache
Memory	32 GB	128 GB
HDD	Boot (500GB, RAID1) + Data (2TB, RAID1)	Boot (4TB, RAID1) + Data (20TB, RAID5)
Bypass Adapter	Yes	Yes
Network Firewall	2 x RJ-45	2 x 10GBASE-SR (850nM)
Network Management	2x RJ-45 (1Gbps)	2x RJ-45 (1Gbps)
Power	740W Redundant	740W Redundant

Minimum System Requirements

CPU

- Intel x86 processors in 64-bit mode

The following CPU features are required to run Indigo SDF

- Intel Streaming SIMD Extensions 4.2 (SSE4.2)
- Popcnt instruction
- Bit Manipulation Instructions (BMI, BMI2)
- Intel Advanced Vector Extensions 2 (Intel AVX2)

Rule of thumb for core requirements is 2 physical cores plus one core for each 1 Gbps traffic.

List of supported NICs chipsets

- Intel 82575
- Intel 82576
- Intel 82580
- Intel I350
- Intel 82599
- Intel X540
- Intel X710

Bypass support

- Silicom Bypass Network Server adapters (Intel-based chipsets only)

Memory

- 16GB RAM for 1 Gbps
- 128GB RAM for 10 Gbps

Storage

- 1.5 GB for Ubuntu Server 16.04 Installation