Network Application Visibility Library (NAVL)

True layer 7 DPI technology for application identification and metadata extraction

NAVL is delivered as an OEM software development kit (SDK) to dramatically reduce the time, cost and complexity of adding DPI technology and application intelligence to your network.

KEY SYSTEM BENEFITS

Advanced DPI technology
- Industry-leading application identification and extraction for greater visibility of Layer 7 traffic

Fast throughput & low memory footprint
- Minimizes impact on network performance and CAPEX requirements

Delivered as SDK
- Rapid, cost-effective network implementation

Real-time identification
- Provides valuable insight into application traffic as it occurs

Easily add deep packet inspection (DPI) technology to enable real-time layer-7 application identification in your broadband network.

Procera's Network Application Visibility Library (NAVL) uses deep packet inspection (DPI) technology to enable real-time, Layer-7 application identification and metadata extraction for network traffic.

NAVL delivers industry-leading network coverage and accuracy, together with the fastest throughput and lowest memory footprint in the market. NAVL uses a combination of deep packet and deep flow inspection techniques to accurately identify more than 1900 complex, rapidly changing and increasingly encrpypted applications, including social networking, P2P, instant messaging, file sharing, enterprise, Web 2.0 applications and tunneling protocols.

SOPHISTICATED IDENTIFICATION TECHNIQUES

NAVL enables a variety of use cases such as analytics, SDWan, security etc., that provide significant benefits to enterprises, cloud and broadband operators, including:

- **Surgical Pattern Matching** – The NAVL engine optimizes pattern matching by selectively identifying contextually relevant patterns at precise locations within each data stream.
- **Conversation Semantics** – NAVL leverages knowledge about how "conversations" occur between networked endpoints to identify and validate application identification.
- **Deep Protocol Dissection** – Going far beyond simple pattern matching, NAVL applies advanced intelligence based on extensive knowledge of transport protocols. This enables it to detect applications attempting to subvert firewall rules by behaving as other protocols.
- **Behavioral & Statistical Analysis** – NAVL calculates and tracks a number of behavioral and statistical markers within each traffic flow. This enables NAVL plug-in modules to use behavioral signatures as part of their traffic identification logic.
- **Future Flow Awareness & Flow Association** – Information extracted and "learned" from one traffic flow is used to improve identification accuracy and efficiency for related flows.
- **First Packet Classification:** NAVL learns from previous flows and it is able to classify future flows going to the same services from packet number one.

NETWORK APPLICATION VISIBILITY LIBRARY (NAVL)

NAVL operates as a user space library and is easily integrated into the host system through defined API calls that provide input and output via packet or data stream interfaces. NAVL is a thread-safe and lock-free library allowing near linear performance scalability to fully leverage the rapid increase in multi-core processor densities. The solution is also customizable with a Packet-based or Stream-based interface and optimized connection management.

NAVL RESULTS

Traffic identification results are returned as an application full stack that will contain application and protocol IDs. Separately, metadata can be returned on current flows. Examples include:

- http.url
- http.host
- http.content_type
- pop3.from
- query.sip.caller.sip
- tls.hostname
- tls.cert
- myqsl.handshake
- vxlan.header

Metadata & Content Extraction

Call-back-driven architecture provides realtime configuration on metadata and content elements

Extensive list of metadata elements can be accessed, including details related to application content type, user information, application performance, VOIP, video quality, and many detailed elements.

Performance

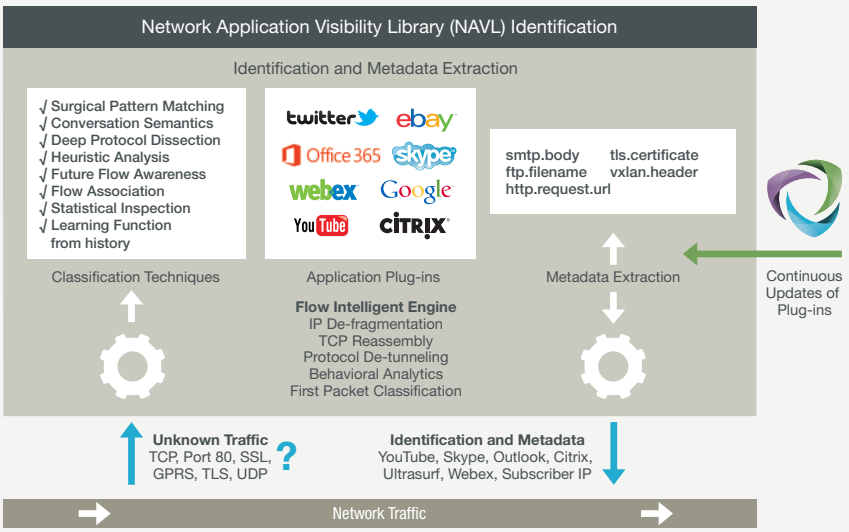
Low memory footprint allowing integration into wide range of hardware platforms, from small, embedded devices from small, embedded devices (like NG firewalls or IoT devices) to bigger appliances (like cloud or SDN solutions).

Performance: 10Gbps per core throughput in a standard x86 environment.

Memory:
12MB base + 1MB per thread + 1KB per flow

Figure 1

NETWORK APPLICATION VISIBILITY LIBRARY (NAVL) IDENTIFICATION



v20170626

ABOUT PROCERA NETWORKS

Procera Networks, the global Subscriber Experience company, is revolutionizing the way operators and vendors monitor, manage and monetize their network traffic. Elevate your business value and improve customer experience with Procera's sophisticated intelligence solutions.
For more information, visit proceranetworks.com or follow Procera on Twitter at @ProceraNetworks.

PROCERA

CORPORATE OFFICES
Procera Networks, Inc.
47448 Fremont Blvd Fremont,
CA 94538
P. +1 510.230.2777
F. +1 510.656.1355

CORPORATE OFFICES
Procera Networks
Birger Svenssons
Väg 28D 432 40 Varberg, Sweden
P. +46 (0)340.48 38 00
F. +46 (0)340.48 38 28

ASIA/PACIFIC HEADQUARTERS
Unit B-02-11, Gateway Corporate Suite,
Gateway Kiaramas
No. 1, Jalan Desa Kiara,
Mont Kiara 50480 Kuala Lumpur,
Malaysia

Copyright © 2017 Procera Networks. All rights reserved. All other trademarks are property of their respective owners.