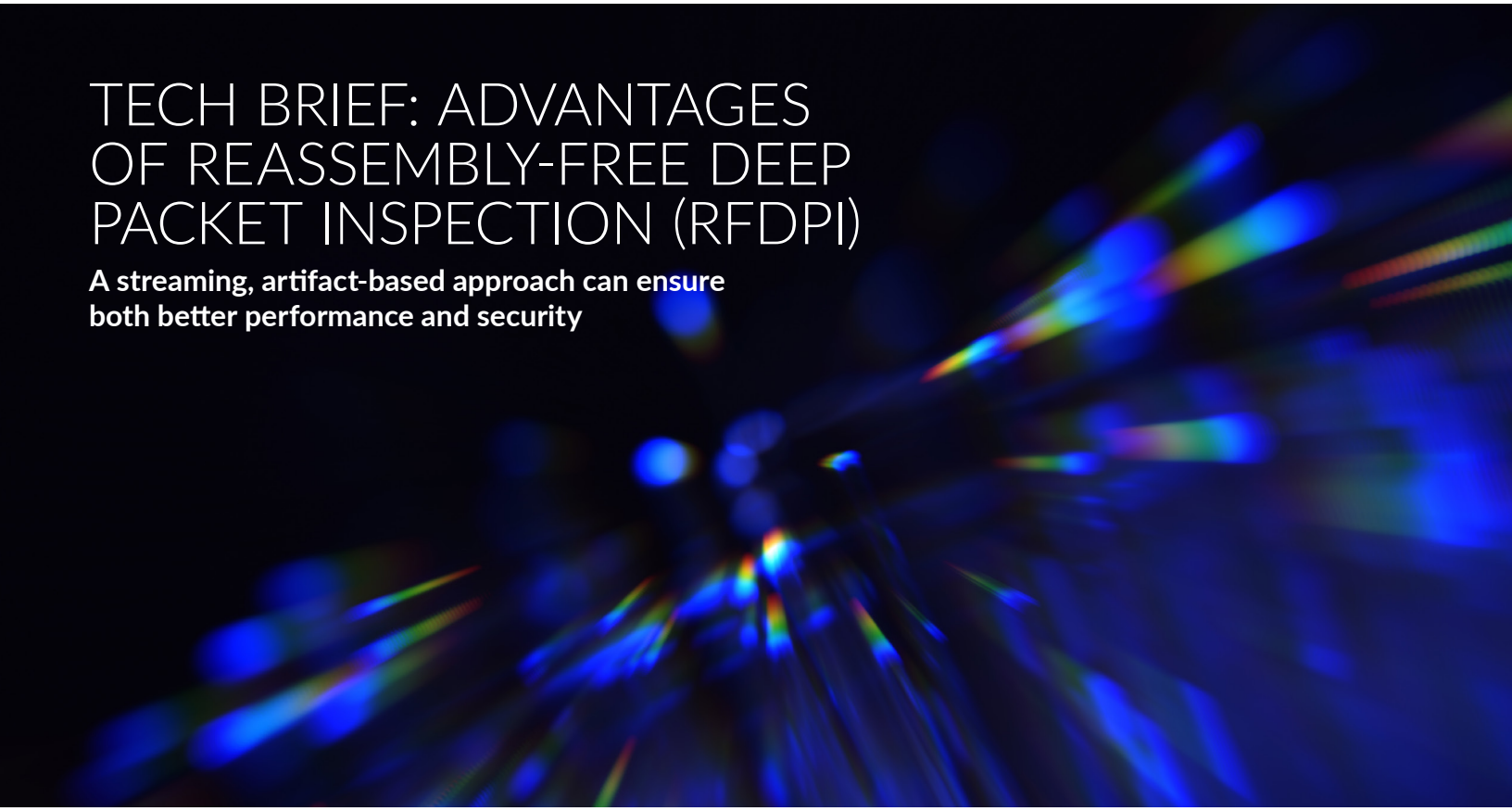
SONICWALL

TECH BRIEF: ADVANTAGES OF REASSEMBLY-FREE DEEP PACKET INSPECTION (RFDPI)

A streaming, artifact-based approach can ensure both better performance and security



Abstract

Proxy-based inspection requires entire malware files to be buffered in memory. A streaming, artifact-based approach, such as SonicWall RFDPI, ensures effective security analysis of every bit of traffic in real time without added latency.

Introduction

The evolving nature and delivery schemes of viruses, malware and spyware have radically changed the scope and best practices of network security. Data inspection at the application-content level is necessary to protect against sophisticated hacking schemes. In the pursuit of application-level protection, Deep Packet Inspection (DPI) has become the preferred approach. There are two core DPI approaches: proxy-based and stream-based DPI.

Both focus on delivering robust network protection via application-level inspection and scanning. However, they have fundamentally different ways of solving the problem, each with a distinctly different impact upon network latency and performance.

Proxy-based inspection

Application proxies operate by breaking the TCP/IP communication between a client and server when a request is passed. The application proxy receives and buffers the entire request, inspects the request and then creates a new connection to the server. This scheme inserts DPI between the endpoints of the connection and increases the level of network protection. However, proxy-based DPI works one application-level request or response at a time — and each one, in a typical enterprise application, can span megabytes or gigabytes (in cases of file downloads).

Imagine application content or a large data file as a complete photograph carved into a jigsaw puzzle of packets, which in turn is sent and received at corporate HQ. The application proxy scanner takes each piece of the puzzle, copies it into a separate buffer file and holds all the pieces in that file until the entire jigsaw puzzle can be reassembled — and only then is it scanned for any threats. A proxy-based solution cannot "infer" what the photograph looks like until it is reassembled, or it risks missing key elements of the picture.

As a result of proxy-based DPI, CPU cycles are spent on buffering versus other tasks, and the CPU must multitask and prioritize between several files already buffered for scanning. This introduces very high latency for proxy-based solutions, compounded by ever-increasing amounts of network traffic containing rich content and multiple applications. Because application proxies are application-specific, an unknown application creates a potential security loophole or compatibility issue.

Cybercriminals can also leverage proxy-based memory limitations by sending malware files that exceed the maximum oversize threshold of a proxy-based firewall's memory. If the malware file is larger than the maximum file size for scanning

in memory, it might be simply passed through to the network, depending on firewall configuration.

Stream-based reassembly-free inspection

In contrast, stream-based DPI scans the jigsaw puzzle pieces in order of arrival. There is no limit as to the file size, no maximum oversize threshold, no buffering of packets (except for in the out-of-order case) until they can all be scanned at once. It deems the photograph "threat-free" once it scans the last jigsaw piece, without the need for reassembly (hence the term “reassembly free” deep packet inspection, or RFDPI).

Multiply that capability across the typical flow of network traffic, and the performance benefits of the stream-based approach are easy to grasp. RFDPI is a very low-latency approach and speaks directly to need for speed in network performance.

The ability of reassembly-free inspection to support all communications protocols (not just HTTP/HHTPS, SMPT and FTP) gives it a scalability advantage as well. This makes stream-based DPI not only faster but easier to deploy, manage and update.

RFDPI is more secure when scanning for threats in real-world deployment scenarios. For example, since proxy-based solutions must buffer content completely, there is never enough memory on the device to buffer all content that is downloaded concurrently by all users on the network. The increasingly large file sizes involved in enterprise applications further compounds the problem. Proxy-based solutions must skip scanning some or most of the downloaded content.

An RFDPI approach has proven no less secure than a proxy-based approach, even for file formats that require full buffering before being decompressed. The real-world implementation of high-quality stream-based solutions has demonstrated that they are indeed capable of decompressing most common compression formats without reassembly. By ensuring the broadest possible protocol support and insight into the real nature of potential threats, an RFDPI solution can align both speed and security concerns in a meaningful way.

SonicWall RFDPI

SonicWall™ Reassembly-Free Deep Packet Inspection™ (RFDPI) engine scans against multiple application types and protocols to ensure your network is protected from internal and external attacks as well as application vulnerabilities. Unlike other scanning engines, the SonicWall RFDPI engine is not limited by file size or the amount of concurrent traffic it can scan. By working at the application layer, RFDPI protects against hidden application vulnerabilities that may be inadvertently letting attackers in through an unknown back door.

Our patented RFDPI engine is at the heart of every SonicWall network security solution. This patented technology unifies multiple security functions into a single integrated suite that inspects all files from local, remote and mobile users. This gives network administrators the ability to manage network security simply and cost-effectively. RFDPI increases productivity by allowing IT to create reusable and adaptive policy control. More than simply a security approach, RFDPI incorporates object-based contextual controls over user identity and access, application identity and access, data leakage, network optimization and granular reporting, auditing and forensics.

Artifact-based analysis

To maximize protection, SonicWall RFDPI leverages artifact-based analysis to identify potential threats as it scans the data streaming in real time. Simply put, RFPDI intelligently looks for indicators of malicious behaviors, coding and evasions. Like spotting a “tell” in high-stakes poker, these artifacts enable RFDPI to highly accurately identify malware without having to scan entire files into memory. One analogy might be the accurate fingerprinting the DNA of a criminal from a single hair follicle.

For artifact-based analysis to effectively succeed, it needs to rely on intelligence that is global, comprehensive and up-to-the-moment.

Capture Labs Threat Network

RFDPI leverages the SonicWall Capture Threat Network, which securely monitors and collects information from global devices and resources including:

- More than 1.1 million security sensors in nearly 215 countries and territories
- Cross-vector, threat-related information shared among SonicWall security systems, including firewalls, email security devices, endpoint security solutions, honeypots, content filtering systems and the SonicWall Capture Advanced Threat Protection (ATP) mulit-engine sandbox
- SonicWall internal malware analysis automation framework
- Malware and IP reputation data from tens of thousands of firewalls and email security devices around the globe
- Shared threat intelligence from more than 50 industry collaboration groups and research organizations
- Analysis from freelance security researchers

As a result, the SonicWall Capture Threat Network collects over 100,000 malware samples and blocks over 27 million malware attacks every single day. This threat intelligence is the foundation for the reassembly-free artifact analysis in SonicWall RTDMI.

Controlling applications in the organization

It can be a real challenge for IT administrators to efficiently deliver critical corporate solutions while also contending with employee use of wasteful and often dangerous applications. Critical applications need bandwidth prioritization while social media and gaming applications need to be bandwidth throttled or completely blocked. Legacy stateful packet inspection firewalls used in many

organizations rely on port and protocol; they cannot solve the problem because they are not able to identify applications.

SonicWall RFDPI examines all downloaded, emailed and compressed files at the application layer to protect against the more sophisticated attacks that target application vulnerabilities. Scanning every byte of every packet of all network traffic, SonicWall provides complete application identification and control, regardless of port or protocol, by determining exactly what applications are being used and who is using them. Administrators can easily create bandwidth management policies based on logical pre-defined categories (such as social media or gaming), individual applications, or even users and groups. SonicWall puts the power back in the hands of IT administrators.

Protection against both internal and external attacks

Deep packet inspection scans multiple application types and covers many protocols, including SMTP, POP3, IMAP, FTP, HTTP and NetBIOS. It also scans all network layers. As a result, your network is protected from both internal and external threats. Deep packet inspection scans multiple application types and covers many protocols, including SMTP, POP3, IMAP, FTP, HTTP and NetBIOS. It also scans all network layers. As a result, your network is protected from both internal and external threats.

Conclusion

SonicWall RFDPI leverages intelligent artifact-based analysis to highly effectively identify and stop internal and external threats without increasing latency.

Learn more. Read the 2020 SonicWall Cyber Threat Report.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com