CSPi

APP NOTE

Bro and the
Myricom ARC
Series Adapters

Bro and the Myricom ARC Series – A Strong Defender Against Zero-day attacks

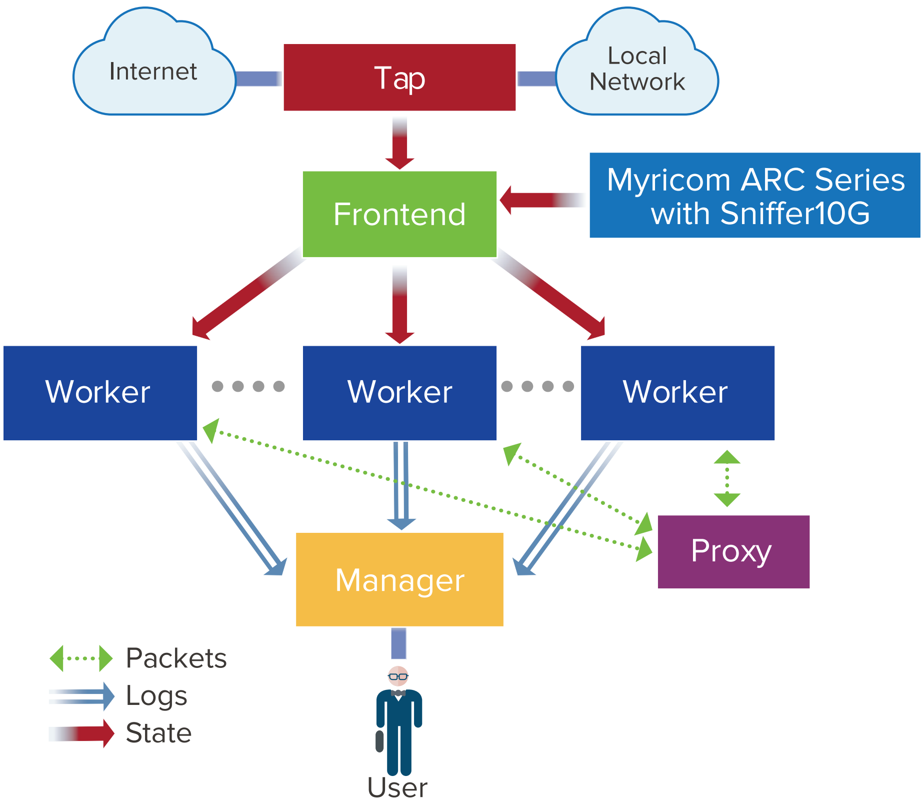
Bro and Myricom
Get the IDS Performance You Need

Bro open source software is a great platform for building a Network Intrusion Detection System (NIDS or IDS.) However, Bro throughput, like that if any IDS, is challenged by ever climbing network bandwidth. It starts with packet capture. At higher bandwidths it is far too easy to drop packets or consume too much CPU time moving packets into Bro through the OS kernel. In addition, higher bandwidths require scaling Bro to use multiple CPU cores. That scaling depends upon specialized, and often costly, hardware or software libraries maintained outside the Bro community.

Fortunately, there is a cost-effective solution to all of these challenges: a Bro plug-in that integrates your application with CSPi's Myricom® ARC Series of network adapters coupled with Sniffer 10G. The plug-in is part of the official Bro distribution and delivers big benefits to Bro users, including:

- **Dropless capture** – Overrunning the capture buffer is the most common cause of dropped packets. Myricom ARC series adapters support the industry's largest capture buffer, providing the best possible tolerance to software performance jitter. Tune Bro to never drop a packet when running against a tap (two 10 Gbit streams merged at line rate.)
- **Reduce CPU usage** – Bypass the OS kernel by sending all packets directly into Bro. This frees up significant CPU cycles for Bro to exploit doing IDS work instead of protocol processing.
- **Scale a single application** – Act as a Bro "front end" by distributing network flows among multiple copies of Bro. BroControl will automatically setup the worker scaling for you.

- **Multiple applications see the same packets** – Simultaneously, run multiple applications along with Bro, such as Snort or Suricata, against the same packets with zero background copying.
- **Improved Forensics** – Some users like to keep a few minutes of packet traffic in a memory buffer which they can snapshot if Bro issues an alert. This is another way to exploit Myricom's ability to send the same packets into two places without making copies.
- **Exact time stamps** – The ARC Series hardware time stamps are very accurate. Bro itself does not require this accuracy but other applications that you may run in parallel with Bro will benefit.



Where to get Bro Plug-in

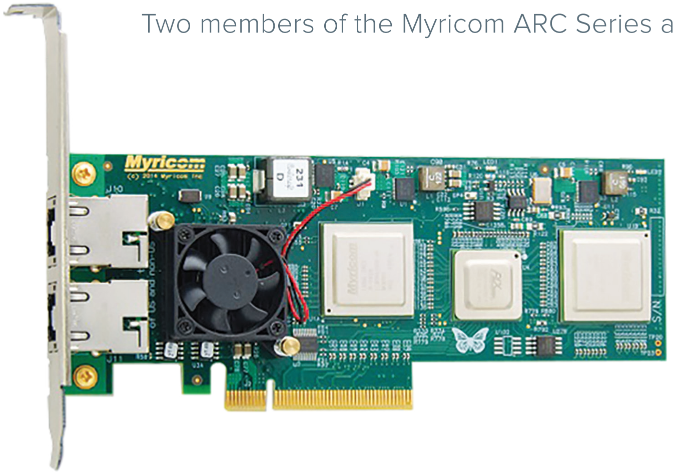
The ARC Series with Sniffer10G Bro plug-in comes as a standard part of the Bro distribution, starting with release 2.4.1. If you are running an older version of Bro, libpcap and even PR_RING acquisition work almost as well. The new plug-in directly leverages our Sniffer10G API. To implement, first you install the Sniffer10G software, then configure Bro using the documentation for the plug-in. To find that documentation, browse to www.bro.org and type "Myricom" into the search box. You will discover many references. The plug-in is named "Bro::Myricom".

Bro open source software focuses on network security monitoring while also providing a platform for more general network traffic analysis. Bro's initial user community included major universities, research labs, supercomputing centers, and open-science communities.

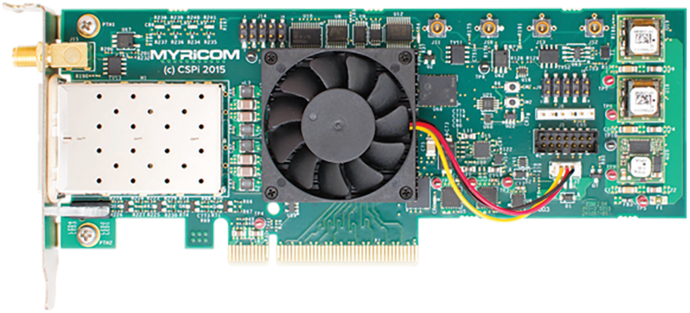
Bro use is rapidly growing to include major corporations seeking to protect themselves from zero-day attacks better than any off-the-shelf, signature-based technology can achieve. See https://www.bro.org

ARC Series Adapters

Two members of the Myricom ARC Series are of particular interest to Bro users:



C-Class – This is our cost-optimized series. It is 10 Gbit only and comes in one or two port versions. There are several form factors including: PCIe low profile, IBM BladeCenter, and an industrial/defense optimized PC/104. The C-series supports both Windows and Linux.



E-Class – This is our feature-oriented series, while still cost optimized. It supports both 1 Gbit and 10 Gbit, 2-port and 4-port. It is PCIe low profile only. There are hardware assists for both merging and RSS to reduce CPU overhead below even the C-Series benchmark. The accuracy of the E-Series timestamps equals that found on much more expensive boards. E-Series is currently Linux only.

Network Intrusion Detection Systems (NIDS) monitor networks, reporting on and responding to malicious activities. They have become essential to every type of system and network, countering cyber-threats that continually grow in both volume and sophistication. NIDS functionality is part of the accepted definition of a “next-generation firewall.” Signature-based IDS systems dominate commercially and were pioneered by the open-source Snort community. Bro is a pioneer in anomaly detection. Many sites run multiple IDS packages to leverage the strengths of each.

Sniffer10G

Myricom ARC Series Network Adapters are supported by Sniffer10G, an integrated combination of hardware and software, optimized for full line-rate packet capture. By simply changing the library you link with, users of libpcap, WinPcap, and PF_RING can leverage CSPi's Myricom Sniffer10G hardware and software. Sniffer10G bypasses the operating system kernel and sends packets directly into user space, leveraging a 'ring' that can expand to any size.

Summary

Working together Bro and the ARC Series provides many benefits not achieved with standard off-the-shelf Ethernet adapters. With the ARC Series and Bro you get a cost-effective way to design a flexible, customized IDS solution that will scale to use all the cores in your server, won't drop packets at full 10 GbE line rates, deliver accurate hardware timestamps, won't overburden your server CPU all while sending the same packets to another Sniffer10G user which could include Snort, Suricata or a packet recorder.

Learn More: To get in-depth details, visit CSPi's website at www.cspi.com/myricom.

Performance Studies

Several organizations have published comments on the performance benefits that ARC Series adapters bring to Bro. Links to these studies are available on CSPi's website at http://lp.cspi.com/Myricom_Bro.html

About CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com
us-hpp-sales@cspi.com

in www.linkedin.com/company/csp-inc
@ThisIsCSPi
us-hpp-sales@cspi.com
www.cspi.com