ixia

WHITE PAPER

SECURITY FORCE MULTIPLIER

Enterprise security isn't a fair fight. A hacker only needs to exploit a single vulnerability, but the enterprise security team must protect every potential attack vector. The statistics reflect the dire situation with the explosion of both new attacks and attack surface:

- Nearly one million new malware threats are released every day[i]
- 71% of exploits are for known vulnerabilities with patches that have been available for a year or more[i]
- Over 1,000 new applications are released every day on Apple's AppStore[ii]

MULTI-VENDOR SECURITY MISHMASH

Security products only focus on specific problems. As a result, enterprise security teams must roll out a number of products to bolster their security. A typical mid-to-large enterprise will commonly deploy a range of tools that include:

- Firewalls and Next Gen Firewalls
- Intrusion Detection Systems (IDS)
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP)

A HACKER ONLY NEEDS TO EXPLOIT A SINGLE VULNERABILITY, BUT ENTERPRISES MUST PROTECT EVERY POTENTIAL ATTACK VECTOR.

The above list looks somewhat manageable, but there is a catch. Within each category of security product, each vendors' solutions are more effective at detecting and preventing different classes of attacks. Security teams maximize their protection by using multiple vendors' products to thoroughly inspect traffic. Effectively, their IDS solution is not a uniform deployment of IDS products from one vendor, but rather an amalgamation of numerous IDS products from multiple vendors. It is often the case that all of these devices require access to the same data.

And the challenges keep growing. Ongoing megatrends such as BYOD (Bring Your Own Devices) invite employees to use their personal devices on enterprise networks. And, more than half of all Internet traffic is now SSL encrypted, hiding threats as effectively as the content. The transition to IoT (Internet of Things) has resulted in numerous companies creating devices built on public domain source code that may or may not be known to be secure.

So what is a security engineer to do?

GETTING THE UPPER HAND ON DATA ACCESS

A force multiplier can tip the tables back in favor of the security engineer. It is unrealistic, in both a practical and financial sense, to expect that every security solution will evolve to access every bit of data. However, judicious use of a visibility and security architecture can dramatically improve the situation by decoupling the security tools from the data access.

MORE THAN HALF OF ALL INTERNET TRAFFIC IS NOW SSL ENCRYPTED, HIDING THREATS AS EFFECTIVELY AS THE CONTENT.

A visibility and security architecture multiplies the effectiveness of security tools by enabling access to data throughout the network using intelligent intermediary devices known as network packet brokers (NPBs) to access and transform the data into a format that one or more security tools can use. For example, a good NPB can:

- Decrypt SSL traffic and feed it as stateful cleartext traffic to one or more security tools
- Identify applications using deep packet inspection, rather than just relying on protocol and port numbers that are easily faked, to send traffic to the best tool for securing a given application type
- Process data flows to remove redundant data, such as duplicate packets that commonly occur when using multiple taps in a network, without losing any of the original information
- Transform data flows from an unsupported format to a form the tool can understand, as is often the case with VNTagged traffic
- Support reliable use of multiple security products in an inline configuration to increase security and to match performance of different devices

CALCULATE HOW AN NPB WILL AMPLIFY SECURITY TOOL IMPACT

The net effect of the above capabilities is to amplify the impact of each individual security tool, allowing it to secure an expanded portion of the network. Consider the example of a typical enterprise network with the following characteristics:

- 25% of the enterprise traffic is encrypted
- There is one duplicate packet for each packet of interest
- 75% of the traffic is tunneled over an unsupported protocol (VNTag, for example)
- 10% of the traffic is simply not interesting because it is used for guest access

A VISIBILITY AND SECURITY ARCHITECTURE AMPLIFIES THE IMPACT OF SECURITY TOOLS SO YOU CAN SECURE MORE OF THE NETWORK.

In the above configuration, the force multiplier for an NPB as described above can be directly calculated by determining the degree of increased coverage available to the security tools. The computation is:

$$Increase = \left(\frac{1}{1-25\%}\right) \times \left(\frac{1}{1-\frac{1}{2}}\right) \times \left(\frac{1}{1-75\%}\right) \times \left(\frac{1}{1-10\%}\right)$$

Increase = 1.33 x 2 x 4 x 1.11

Increase = 11.85 times more visibility

The above is a simple, but realistic example of how a security architecture can directly impact security effectiveness.

Deploying a visibility and security architecture allows security teams to amplify the impact of their security products so they can secure more of the network and begin to tip the scales back in their favor. If you would like to understand how a security architecture applies to your network then please reach out to Ixia and we will help you understand the benefits and risks that apply specifically to you.

IN THE ABOVE CONFIGURATION, THE SECURITY FORCE MULTIPLIER FOR AN NPB = 11.85 TIMES MORE VISIBILITY

i Verizon's 2015 Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/2015/)

ii International Business Times (http://www.ibtimes.co.uk/apple-app-store-growing-by-over-1000-apps-per-day-1504801)

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805

WWW.IXIACOM.COM

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44 1628 408750
(FAX) +44 1628 639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127