



Background Traffic and Network IPS Testing

by

Jack Walsh
Intrusion Detection and Prevention Program Manager
ICSA Labs, a division of Cybertrust Corporation

and

David Koconis, Ph.D.
Technical Lead Network Intrusion and Prevention
ICSA Labs, a division of Cybertrust Corporation

July 5, 2006

Background Traffic and Network IPS Testing

Introduction

ICSA Labs believes that it is essential for Network IPS testing to be conducted with background traffic. This whitepaper explains the reasons why background traffic in Network IPS testing is so important. And the paper explains why the background traffic cannot be comprised of just any mix or limited to just one or a handful of protocols. Also explained is why the Network IPS team at ICSA Labs believes that using packet captures taken from real corporate networks is the most realistic and cost-effective source of background traffic for Network IPS testing.

What is Background Traffic?

Millions of corporate workers sit down everyday at work and send e-mail, browse the web, transfer files, etc. They log into domains, send instant messages, and remotely administer networking equipment. Some have VoIP at work and make their phone calls over the Internet. All this data and more proceeds through various network checkpoints while en route to its destination.

One of the checkpoints is likely to be a Network Intrusion Prevention System (IPS), since a Network IPS sits inline in corporate networks inspecting traffic for various attacks aimed at remotely-exploitable vulnerabilities. All the data being passed back and forth through the Network IPS that is free of attacks is considered "background traffic."

Why Testing With Realistic Background Traffic is Crucial

There are two key reasons that explain why testing Network IPS devices with background traffic are so important. These reasons are as follows:

- Testing a Network IPS without realistic background traffic does not reflect what is seen in the real world where Network IPS engines are deployed.

In the real world, attacks do not occur all by themselves; they happen while in the midst of all sorts of other network traffic. Test results obtained without using an appropriate mix of realistic background traffic might not accurately reflect the behavior of a Network IPS deployed in a real-world network.

- Background traffic consumes Network IPS resources.

Without background traffic, the Network IPS team would not be able to accurately assess how the Network IPS behaves when under any kind of duress. Examples of functionality that may be adversely affected by the level and kind of background traffic present include blocking attacks, the amount of one-way latency introduced by the device, the ability to mitigate DoS attack traffic, and the responsiveness of the management interface.

Consider the increased difficulty of the Network IPS to detect and block attacks as background traffic levels approach the rated throughput of the Network IPS. If background traffic consumes too much Network IPS resources, an insufficient amount of memory resources on the Network IPS may remain to properly reconstruct a malicious session

before an attack signature can fire. In this case, the attack would get through – though it is repeatedly blocked when no background traffic is present.

Because testing with background traffic is so important, several requirements in version 1.0 of the *Network IPS Corporate Certification Testing Criteria* refer to filling 80% of the bandwidth with background traffic. For example, the bandwidth must be largely consumed as the candidate prevents attacks targeting vulnerabilities in the vulnerability set, and while mitigating trivial DoS attacks, and when determining the amount of one-way latency introduced by the candidate Network IPS.

Characterizing the Background Traffic

There are several different characteristics that can be used to describe the background traffic on a network including the:

- Percentage of one protocol versus another – as indicated by the protocol field in the IP Header (e.g., 6 = TCP, 17 = UDP, etc.);
- Percentage of each application layer protocol (e.g., HTTP, SMTP, DNS, etc.);
- Average frame size – with 1518 being the largest possible Ethernet frame size;
- Average number of TCP and UDP sessions¹;
- Average number of new sessions per second;
- Average data rate.

When ICSA Labs began its research to develop a program to test network intrusion prevention systems, the Network IPS team took steps to ensure that the mix of background traffic used in testing would be representative of what a corporate end user would see in the network locations where a Network IPS engine was deployed. To accomplish this, the Network IPS team researched the protocol composition of traffic at Internet connections and at the core of an organization's network.

Generally, the research produced no conclusive result. For example, the Network IPS team found no definitive information characterizing the traffic mix at the core of a corporate organization. In contrast, there were a handful of Internet-related traffic studies performed by organizations like CAIDA². However, the information did not reflect the present-day Internet and did not contain data taken from many corporate organizations across a variety of different vertical markets.

When the research lead to a dead end, the Network IPS team solicited information from Network IPS Product Developers (NIPD) consortium members. NIPD members were normally well-versed in the traffic characteristics of the organizations deploying their products. ICSA Labs worked to come up with background traffic mixes aligned with the general NIPD member guidance summarized in the bulleted items below:

- Reflect the traffic mixes seen in corporate organizations in those locations where Network IPS devices are deployed;
- There should be much more TCP than UDP traffic in terms of both packets and bytes;

¹ We use the term “sessions” loosely when talking about UDP, since it is a “connectionless” protocol.

² One of the papers reviewed was the, “Longitudinal study of Internet traffic in 1998-2003” by Fomenkov, Keys, Moore, and Claffy. It is available at:

http://www.caida.org/publications/papers/2003/nlanr/nlanr_overview.pdf.

© Cybertrust 2006. All rights reserved. Cybertrust and ICSA Labs are registered trademarks of Cybertrust Holdings, Inc. and/or its affiliates. All other trademarks are property of their respective owners.

-
-
- A typical average frame size for Internet traffic was approximately 400-550 bytes;
 - HTTP is the predominant protocol on the Internet.

Additionally, the Network IPS team chose background traffic mixes that would challenge devices optimized (or not optimized) for either one or some number of application layer protocols. This was in response to learning from a Network IPS developer that the code path for an older iteration of their product was significantly faster when inspecting one particular protocol than the code path for inspecting the thousands of other possible protocols. Once updated and improved their product no longer handled other protocols so much more slowly. The Network IPS team recognized that it might be possible to expose any such limitations in candidate Network IPS engines during testing through the use of varied mixes of realistic background traffic.

Background Traffic Source

The Network IPS team considered three sources for background traffic. The first was to use commercial or free traffic generation tools such as those produced by Agilent, IXIA, and Spirent. The second was to build a network that included a varied set of real clients and servers. And the third option was to replay packet captures taken from actual corporate networks.

The Network IPS team saw strengths in all three approaches. In fact, ICSA Labs has prior experience with the first two background traffic sources. ICSA Labs has successfully used traffic generation tools in other labs for testing. Also, the former ICSA Labs network intrusion detection systems program built a network that simulated the behavior of a real network. Operated by sophisticated scripts that were written to control various real clients and servers the simulation network moved generic traffic and specific types and sets of data back and forth in order to create useful background traffic.

Though there are merits to these approaches for the purposes of Network IPS testing, both were limited in terms of:

- Available application layer protocols – One particular traffic generation tool can generate background traffic for 10 application protocols. However, with literally thousands of application layer protocols the Network IPS team did not want to be limited to a relatively small percentage of protocols, even though one of the protocols frequently implemented in traffic generation tools is HTTP, which accounts for a large percentage of Internet traffic. ICSA Labs understands that Network IPS devices will be deployed in all sorts of networks at several different locations within the network (i.e., not just at the Internet perimeter) and will therefore be exposed to traffic from far more than 10 different application protocols. Further, creating a network that generates background traffic and attempts to mimic many different kinds of protocols falls far outside of the boundaries of what can be built cost effectively.
- Real mixes of corporate traffic – The Network IPS team worked to be sure that the traffic generated for testing was realistic both in terms of the mix of protocols and in terms of the content. Consider just HTTP; it is not clear that a tool or simulation network could ever realistically recreate the richness, complexity, and variety present in HTTP GET or POST requests. For example, passing long and sophisticated cookies, or php session variables, or other similar variables – so long in fact that the requests are passed in multiple frames – is not readily or realistically simulated.

Ultimately, the Network IPS team believed that replaying once-live packet captures – if it could be done correctly – would be the most realistic means to produce background traffic for Network IPS testing. This was because packet captures taken from real, corporate networks are comprised of traffic that really happened. Unlike the other two techniques, the traffic from packet captures is not contrived in any way, shape, or form. Further, replaying packet captures was cost effective. There was no need to create a lab with real P2P, Oracle, Tivoli, SAP, and other network clients, servers, and databases. The obvious questions were could ICSA Labs get useful packet captures from corporate networks to serve as background traffic for Network IPS testing and could they be replayed properly?

Fortunately, unlike other testing organizations, ICSA Labs has two unique sources of information. In addition to the consortium of Network IPS developers that provide a wealth of information, ICSA Labs has relationships with an internationally-diverse set of corporate and government organizations. These relationships formed over time by virtue of being a division of a mid-sized, global information security company and by virtue of being the de facto standard in computer and network security certification testing for over 15 years.

As a result of these relationships, the Network IPS team was in a position to ask corporate customers for packet captures from their networks. Before the initial round of testing began in earnest the Network IPS team began filling a database repository that now contains several hundred gigabytes of corporate packet captures – primarily from Internet links, co-location facilities, and the core of corporate networks.

Building this packet capture repository is an ongoing activity. It has to be a continuous process because networks change over time as does the composition of traffic on these networks. As an example, consider the increase over the past several years in the different kinds of P2P application traffic on the Internet (e.g., Bit Torrent, eDonkey, Kazza, WinMX, etc.). Thus, the Network IPS team will continue to target corporate organizations across a number of vertical markets. The goal then is to continually add to the ICSA Labs database repository of packet captures, producing a robust set of packet captures that remain relevant and useful as background traffic in Network IPS certification testing.

Using Packet Captures for Background Traffic

Using packet captures presents some unique challenges.

One issue was that packet captures are not likely to be “clean.” In other words, the Network IPS team could not just take a packet capture, once received, and begin replaying it on the test network without first checking to see if any traffic should be removed from it. For example, the Network IPS team obtained several packet captures where only the first X bytes of each frame were recorded. Thus data was missing for all those frames in the packet capture that were originally greater than X bytes. In such cases, the offending frame(s) and corresponding session(s) were removed in an effort to avoid increases in latency and decreases in throughput, and also to avoid potential false positives due to shortened, unusual frames.³

Once cleaned, the network IPS team had to determine which resulting packet capture still had the characteristics of one that ICSA Labs could use. Though the Network IPS team had hundreds of gigabytes of packet captures in its database, a limited number of packet captures –

³ Because the pre-testing step to clean packet captures was so involved it is itself the topic of an upcoming whitepaper.

© Cybertrust 2006. All rights reserved. Cybertrust and ICSA Labs are registered trademarks of Cybertrust Holdings, Inc. and/or its affiliates. All other trademarks are property of their respective owners.

once clean – still had an acceptable protocol mix in terms of TCP and UDP, percentage of HTTP compared to other applications, and average frame size. For example, the average frame size for one packet capture dropped to about 300 bytes, smaller than the targeted 400-550 byte range.

The final hurdle in using packet captures was finding an appropriate means by which to properly replay them in the Network IPS test lab. Of major importance was the fact that the replay tool had to be able to generate multi-gigabit per second throughput since several Network IPS devices were rated for 1+ Gbps.⁴ Two other primary concerns with replaying a packet capture are that there needs to be some way to:

- ensure that packets coming from a particular client IP always pass through the candidate Network IPS in the same direction (beginning and ending with the same interfaces) and that packets returning from a particular server IP always pass through the same, but opposite interfaces of the client traffic when returning to the client, and
- ensure that responses are never sent until the frame that elicited them is first received.

An open source tool called Tomahawk, originally developed by a Network IPS developer, was the solution to these concerns. Both because of its birth through a Network IPS developer and also due to a number of known shortcomings, some Network IPS developers had reservations about its use by ICSA Labs. However, since Tomahawk was open source the Network IPS team both corrected the known problems and also made numerous other improvements that largely alleviated those reservations.⁵

Summary

When deployed, a Network IPS has to be able to prevent attacks while in the midst of attack-free traffic, called background traffic. Therefore, the Network IPS team at ICSA Labs recognized that testing without background traffic would not be realistic. After research performed by the Network IPS team failed to reveal what comprised a “normal” mix of traffic both on the Internet and at the core of corporate organizations, ICSA Labs decided to follow some general guidelines given by Network IPS developers, based on first-hand knowledge of their products’ deployments. After considering three options to generate the background traffic that conformed to these guidelines, the Network IPS team pursued and obtained packet captures from the Internet perimeter and the core of various corporate organizations. The packet captures taken from these networks, unlike background traffic from other sources, did not contain an artificially restricted protocol mix and was in no way contrived. The Network IPS team transformed the packet captures through some serious cleaning into the background traffic that was used for Network IPS certification testing.

Biography

Jack Walsh, Intrusion Detection and Prevention Program Manager

Before coming to ICSA Labs, Jack Walsh worked at the National Security Agency (NSA) for 8 years primarily as an evaluator in the Trusted Product Evaluation Program. While at NSA, he

⁴ Recall that the Network IPS team had to be able to generate 80% of the rated throughput claimed by the developer. Therefore if the developer claimed 10 Gbps throughput, while enforcing a policy that met the criteria then ICSA Labs would crank up the throughput to 8 Gbps.

⁵ For a list of the improvements that ICSA Labs made to Tomahawk, refer to <http://tomahawk.sourceforge.net/>. From there select the link, “Changes from 1.0 to 1.1.”

© Cybertrust 2006. All rights reserved. Cybertrust and ICSA Labs are registered trademarks of Cybertrust Holdings, Inc. and/or its affiliates. All other trademarks are property of their respective owners.

helped author the first-ever US Government Firewall Protection Profile. Since then he has worked 8 years at ICSA Labs. He was the Technical Lead in the Firewall Lab for over 4 years before being named Program Manager for the Network IPS Certification Testing Program. Jack earned his B.S. in Electrical Engineering from The Pennsylvania State University and his M.S. in Computer Science from Johns Hopkins University.

David Koconis, Ph.D., Technical Lead Network Intrusion and Prevention

David Koconis joined ICSA Labs in July 2005. Prior to joining ICSA, he worked at the Institute for Security Technology Studies at Dartmouth College where he managed and was the lead developer of the Security Cybersleuth, a web-based service that collects and indexes computer security related information from open sources on the Internet. He is also a co-author of "Securing Linux-A Survival Guide for Linux Security" (ISBN: 0974372773). David earned his B.S. degree in Aerospace and Ocean Engineering from Virginia Tech and his M.S. and Ph.D. in Aeronautics and Astronautics Engineering from Stanford University.

Acknowledgements

The authors would like to acknowledge the ICSA Labs team for reviewing and providing input into the content of this document.

Who To Contact At ICSA Labs

For questions or comments about this paper contact Jack Walsh at jwalsh@icsalabs.com or David Koconis at david.koconis@icsalabs.com. For more information regarding the ICSA Labs Network IPS Certification Testing Program or Network IPS Product Developers (NIPD) Consortium, visit www.icsalabs.com and follow the "Network Intrusion Prevention" hyperlink.

About ICSA Labs

ICSA Labs, an independent division of Cybertrust, Inc., offers vendor-agnostic testing and certification of security products. Hundreds of the world's top security vendors submit their products for testing and certification at ICSA Labs. The end-users of security technologies rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. The organization tests products in key technology categories such as anti-virus, anti-spyware, firewall, IPsec VPN, cryptography, intrusion prevention, PC firewall, SSL-VPN, application firewall, anti-SPAM and Wireless LAN. For more information about ICSA Labs, please visit: <http://www.icsalabs.com>.

About Cybertrust

Cybertrust is the global information security specialist, delivering services that secure critical data, protect identities and help customers demonstrate ongoing compliance. Headquartered in Herndon, Virginia, United States, with more than 30 offices around the globe, Cybertrust is one of the world's largest providers of information security and is recognized as the global market leader in managed security services. For more information, visit www.cybertrust.com.