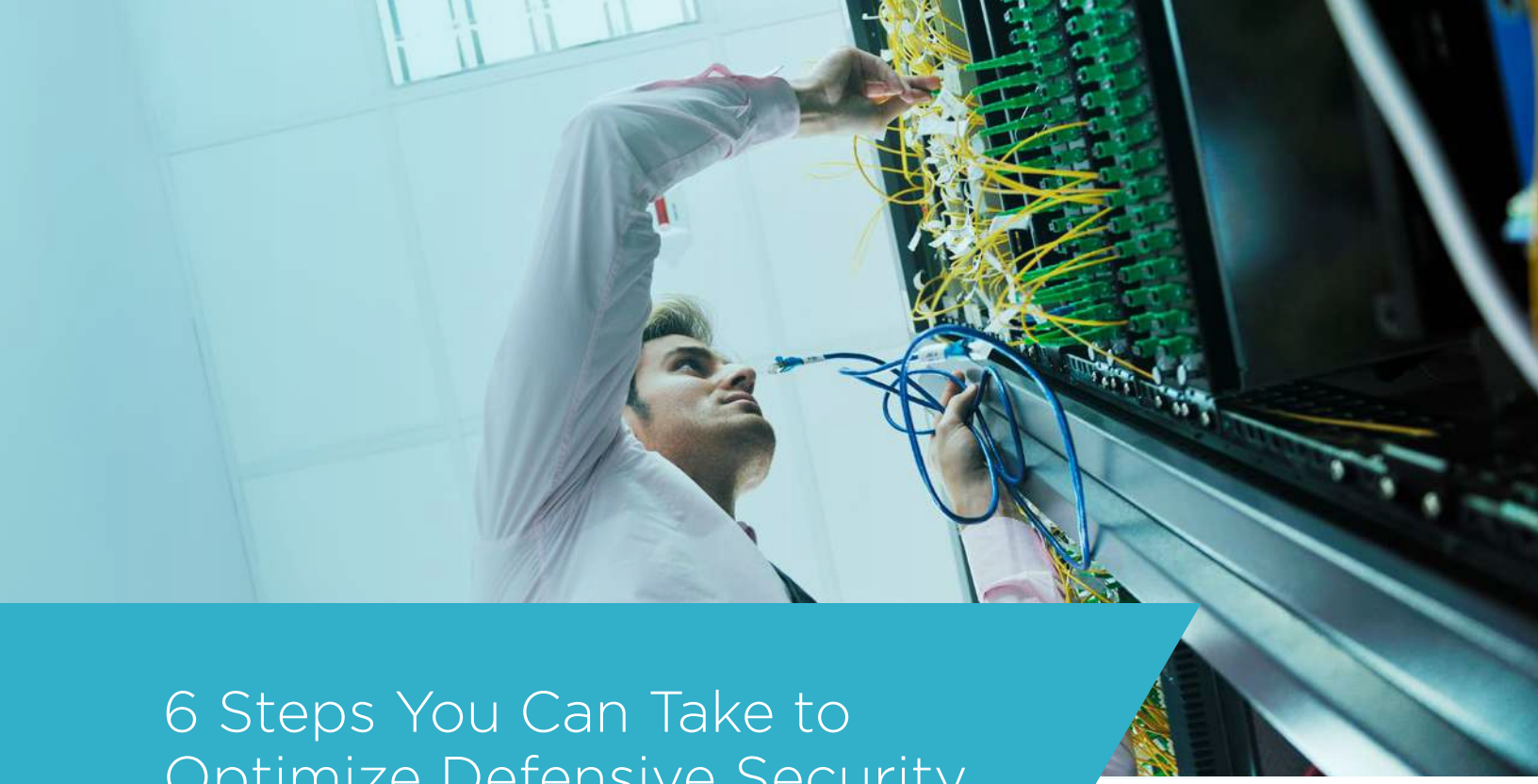

# 6 Steps You Can Take to Optimize Defensive Security

WHITE PAPER

## A SIX-STEP APPROACH TO OPTIMIZE ENTERPRISE SECURITY

According to Radware, 93% of companies experienced a cyberattack in the last twelve months.[1] Amongst the many security strategies available to security architects, a defensive approach is one fundamental strategy that stands out. The defensive approach focuses on preventing as many breaches as possible.

Most businesses already focus on a defensive approach. However, defensive security implementations can be very complex, with conflicting and overlapping tactics. A simple approach that allows you to play both defense and offense will give you an advantage against bad actors, yielding superior results.

Here is a six-step approach for securing your enterprise:

1. Validate equipment readiness against malware and distributed denial of service (DDOS) attacks with a security threat tester
2. Block traffic from known bad IP addresses
3. Use inline real-time traffic analysis to search for hidden malware and security threats
4. Decrypt data packets for better security inspection
5. Perform advanced data filtering to improve analytics
6. Enable deep packet inspection for threat detection and analysis

A simple approach that allows you to play both defense and offense will give you an advantage against bad actors.

ixia
A Keysight Business

[1] The Trust Factor – Cybersecurity's Role in Sustaining Business Momentum, Radware. January 2019.

## 1. VALIDATE YOUR EQUIPMENT READINESS

As a security engineer, you should begin by investigating the equipment already deployed in your network, testing it against various security threats. Obvious threat examples include DDOS and malware. You need to understand the capabilities of your defenses, and their strengths and weaknesses. Component testing in this manner is different from network penetration testing and port scanning activities.

To accurately test your equipment, you will need a combined traffic and malware generator. This test device will create simulated traffic to mimic the type and amount of load on your network. The tester can then launch DDOS and malware attacks against your network components to see how well the security equipment handles the threats under load.

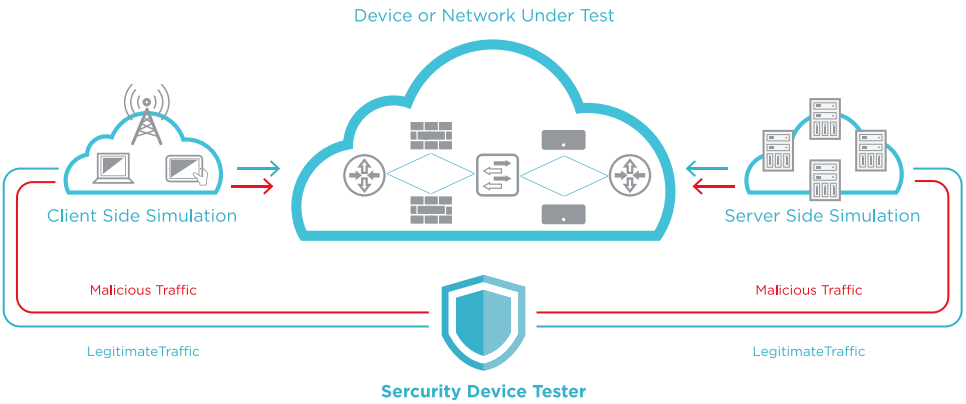


Figure 1. Step 1: Equipment validation against security threats.

This type of testing typically results in the observation that most security devices do not function according to manufacturer specifications for throughput. Actual performance numbers, according to Ixia research, are typically 20 to 30% lower than manufacturer specifications. This is because the security device tester creates a real-world environment, not an ideal lab environment. One note, the malware and DDOS attacks created by the test unit are real. So only perform this type of testing in a lab environment unless you want to take your production network out of service.

## 2. BLOCK TRAFFIC FROM KNOWN BAD IP ADDRESSES

Once you know the performance of your devices, the second step involves reducing incoming threats. Specifically, you want to block traffic from known bad IP addresses. Threat intelligence gateways that provide blocking capability are a perfect choice. Firewalls perform this capability as well, but the key is to eliminate any manual intervention on your part. You want to minimize time spent configuring firewall access lists to block constantly changing IP addresses.

Security device testing typically results in the observation that most security devices do not function according to manufacturer specifications for throughput. Actual performance numbers are typically 20 to 30% lower than manufacturer specifications.

Threat intelligence gateways with automated blacklists eliminate up to 30% of incoming threats right away, reducing your company's risk, according to Ixia research. Since most of this traffic is flagged as suspicious activity on your intrusion prevent system (IPS), you can expect a nearly 30% reduction in false positives on your IPS equipment as well. This reduces alert fatigue and speeds up IPS alert follow-throughs.

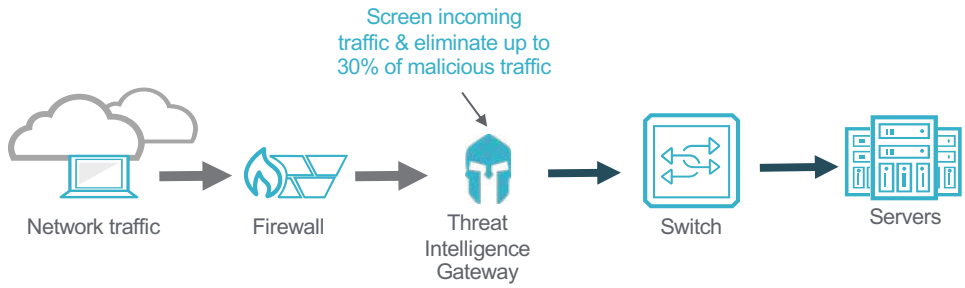


Figure 2. Step 2: Eliminate traffic from known bad IP addresses.

## 3. ANALYZE TRAFFIC WITH INLINE SECURITY APPLIANCES

Implementing an inline security tool solution for real-time analysis of incoming traffic that looks for hidden malware and security threats. Inline security tools (IPS, web application firewall (WAF), unified threat management (UTM), and others) allow you to proactively stop malicious threats before they enter the core network.

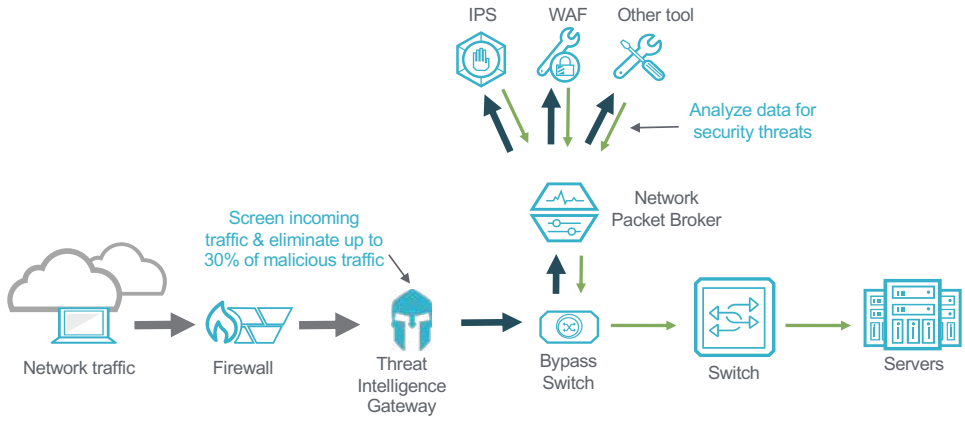


Figure 3. Step 3: Deploy inline security tools to analyze traffic for threats.

A standard inline tool deployment creates a single point of failure. This will do as much damage as a hacker—it will stop all incoming (and potentially outgoing) data flow on your network. A bypass switch deployed after the firewall allows your tools, such as your network packet broker and inline security tools (IPS, etc.), to operate without putting the network at risk.

All traffic that reaches the bypass switch is shunted off to the NPB where it can be filtered, and load balanced to the security tools to create (n+1) survivability. Heartbeat messaging deployed between the bypass and NPB, and NPB to the security tools, provides another layer of reliability and business continuity.

All traffic that reaches the bypass switch is shunted off to the NPB where it can be filtered and load balanced to the security tools to create (n+1) survivability. Heartbeat messaging deployed between the bypass and NPB, and NPB to the security tools, provides another layer of reliability and business continuity.

## 4. DEPLOY DATA DECRYPTION

The Secure Socket Layer (SSL)/transport layer security (TLS) protocol protects network data from unauthorized visibility. Unfortunately, hackers have adapted to encryption as well, and now hide their malware within encrypted data packets. Encrypted malware attacks are increasing at a rate of 30% or more per year.[2]

In addition, many tools cannot process encrypted data. The solution is to decrypt data packets, so security appliances can perform better security inspection. According to a recent EMA survey, 73% of security professionals are looking at decryption to help them secure their networks.[3]

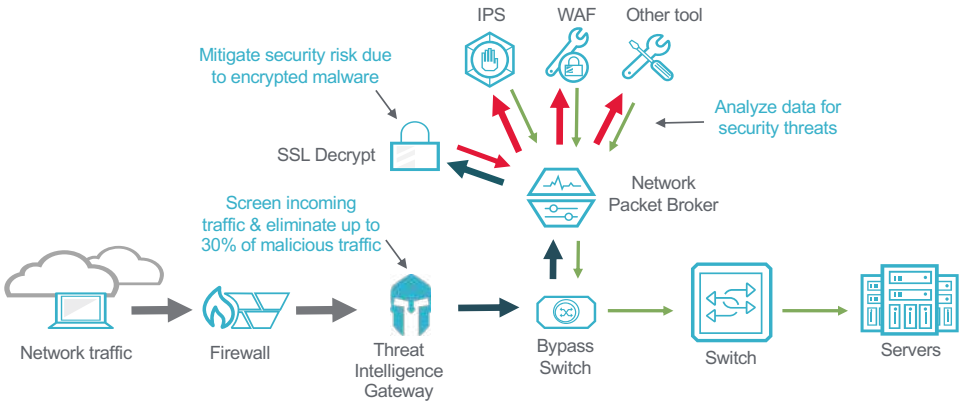


Figure 4. Step 4: Deploy data decryption to find hidden threats.

Once an NPB is deployed, there are two ways to perform decryption. One way is to connect an SSL decryption appliance to an NPB for high volume data decryption. Decrypted data is relayed back to the NPB, which will forward the data to the correct security appliance for analysis. The alternative is an integrated decryption approach where the NPB performs the decryption process. The NPB will forward the data directly to special purpose tools without impacting application performance. Data that passes analysis is re-encrypted and sent to the network core.

## 5. PERFORM ADVANCED DATA FILTERING

The amount of data on your network will triple between 2016 and 2021, and so will your costs to analyze all that data.[4] You will need more security tools and time to sift through the results. A more efficient and cost-effective approach involves isolating data that has a higher probability of being a security threat and analyzing just that data. This advanced filtering approach allows you to

The amount of data on your network will triple between 2016 and 2021 and so will your costs to analyze all that data. This will require a lot of security tools and a time-intensive effort to sift through the results.

A more efficient and cost-effective approach is to isolate data that has a higher probability of being a security threat and analyzing just that data.

[2] Zscaler SSL Threat Report, Zscaler. February 2018

[3] Report Summary: TLS 1.3 Adoption In The Enterprise, Enterprise Management Associates, January 2019.

[4] The Zettabyte Era: Trends and Analysis, Cisco Systems.

cost-effectively scale your security solution. An NPB with application intelligence provides the capabilities necessary to perform this task.

Investigating application data starts with identifying the types of application data that should be inspected and shunting it to your security tools. This involves deploying a network packet broker with application filtering and advanced data analytics to detect suspicious activity.

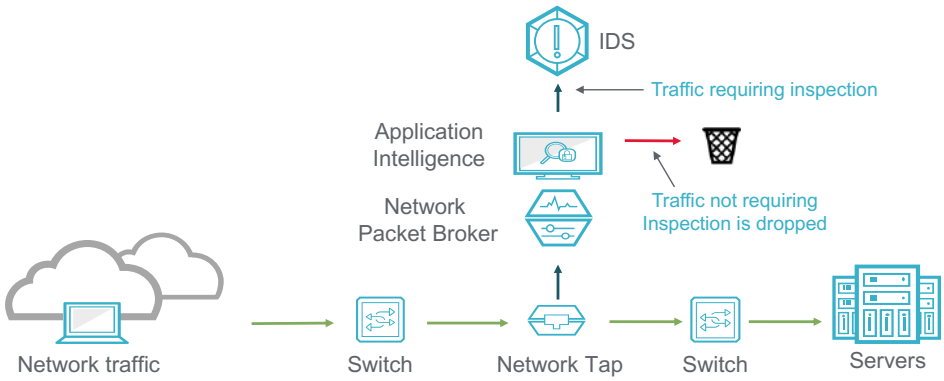


Figure 5. Step 5: Perform advanced data filtering to remove low threat data.

Figure 5 shows the out-of-band version of the inline use case shown earlier. A typical NPB will only focus on layer 2 through 4 packet data, directing data to security tools based on basic parameters. An advanced NPB uses Layer 7 data, adding contextual information based upon application type and routing information to provide another layer of screening intelligence.

For example, take a university that has extensive amounts of data flowing across its network for research — file transfers, communications (voice and email), and video (video conferencing, as well as streaming apps for students living on campus). Screening all this data would take a long time and a lot of security tools. At the same time, some audio information (like voice over IP (VoIP) and Pandora), and video information (like Hulu, Netflix, and Amazon) may not be worth screening. By using application intelligence, an NPB could look at the data based upon application type and filter this type of data out of the monitoring data analysis stream. Data that requires further analysis passes on to an intrusion detection system (IDS).

Employing an application filtering approach can reduce the amount traffic sent to an IDS by up to 35% [5] , providing significant cost savings to the university IT staff. The university literally cuts its IDS tool costs by one-third.

Employing an application filtering approach can reduce the amount traffic sent to an IDS by up to 35%, providing significant cost savings to the university IT staff. The university literally cut its IDS tool costs by one-third.

[5] University of Texas Secures Network While Controlling Costs, Ixia, a Keysight Business.

## 6. ENABLE DEEP PACKET INSPECTION

Use deep packet inspection (DPI) to find real security threats buried in normal traffic flows.  DPI goes far beyond simple detection of patterns, performing forensic analysis to see data exfiltration attempts and limiting data loss.

Taps and NPBs capture either widespread network data and/or very granular pieces of network data, and then distribute that data to various security tools, like a data loss prevention (DLP), next-generation firewall (NGFW), or IDS for analysis.

Well-designed NPBs allow information technology (IT) engineers to selectively screen packet data based on various criteria, like routing protocol, IP address, VLAN, application type, or other parameters, and deliver that data to the security tools, e.g., a DLP, for deep packet inspection. DLPs then extensively review suspect data, analyze the data, formulate a determination, and pass that information on to other devices.

In addition, NetFlow data can be delivered to security and analysis tools, like a security information and event management (SIEM), for analysis and security decisions. The SIEM either quarantines the information or delivers it to a storage device so that an IT engineer can review the data as part of a possible breach and remediate the threat.

Taps and NPBs capture either widespread network data and/or very granular pieces of network data, and then distribute that data to various security tools, like a DLP, next-generation firewall (NGFW), or IDS for analysis.

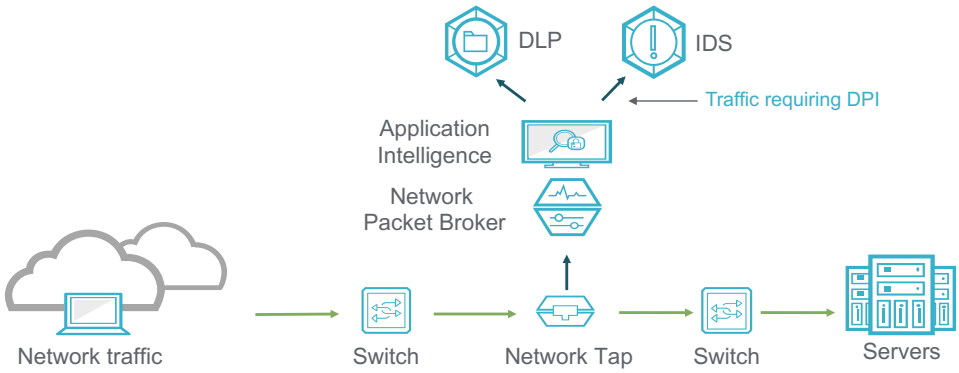


Figure 6. Step 6: Enable deep packet inspection.

## CONCLUSION

When it comes to ensuring network security, the deck is stacked against you. Bad actors have access to low cost, high impact security attack tools. You need to be able to play both defense and offense to keep up the defenses against them.

The six-step approach provided helps you maximize the security of your enterprise:

1. Validate your tools are ready to face malware and DDoS attacks by using a security test tool
2. Block: Traffic from known bad IP addresses
3. Analyze: Real-time traffic for hidden malware and security threats
4. Decrypt: Data packets for better security inspection
5. Perform: Advanced data filtering to improve analytics
6. Enable: Deep packet inspection for threat detection and analysis

Ixia network visibility solutions give you every advantage against hackers, helping you optimize your network monitoring architecture while strengthening network security.

For more information on network monitoring solutions, visit www.ixiacom.com/solutions/network-visibility.

Bad actors have access to low cost, high impact security attack tools. You need to be able to play both defense and offense to keep up the defenses against them.

## Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info



915-9354-01-5091 Rev A 