WHITE PAPER

Inline Security and Why You Need It

Security is now a boardroom topic for every business. It has become one of the most important areas of executive concern because of its ability to:

- impact revenue
- increase corporate risk
- adversely affect customer satisfaction
- jeopardize regulatory compliance initiatives

At the same time, how do you translate these goals into a realistic and achievable security architecture? Inline security solutions are one way that organizations can address this question. The *solution* is more than just adding an inline security appliance, like an intrusion protection system (IPS) or a web application firewall (WAF). It requires complete data visibility, which allows examination of all data for suspect network traffic.

This white paper will:

- summarize the market drivers for inline security
- show how an inline architecture solves common security problems
- provide an overview on how to implement inline security

KEYSIGHT TECHNOLOGIES

Inline Security Market Drivers

According to the latest World Economic Forum report on global risks, cyberattacks and data fraud / theft are now two of the top five risks that CEOs face.[1] This has led to a reprioritization of enterprise objectives and spending. Data from Forrester Research shows that the following are businesses' top security priorities for the next 12 months (as of January 2019).[2]

1. improve advanced threat capabilities
2. improve return on security investments
3. simplify security environment
4. increase productivity of security staff
5. improve operational efficiency

Translating the list above into actionable insights yields the following points:

- Cyberattacks and security incidents are prevalent and costly.
- Security tool failures can cause network and application downtime.
- Successful security monitoring depends on complete visibility.
- Simplicity helps control cost.

Network security has been a topic of discussion in corporate boardrooms since at least 2015. To address the risk presented by security threats, businesses are strengthening their security systems and processes.

However, for a business to be truly successful at achieving these goals, it needs to translate them into actionable insights that allow for the re-architecture of the business' security network. This will not be an easy task. The good news is that technology is available to help businesses create the right security architecture to address these goals, along with unforeseen sources of risk. The next section will provide generalized insight to help solve the problem.

The need for an inline security solution

Organizations are finding themselves fighting security battles on many fronts: an increase in the velocity and variety of cyberattacks, an increase in the number of alerts they need to investigate, malware camouflaged in encrypted traffic, and breaches that are harder than ever to spot. Each of these threats can have a significant impact on the bottom line.

1. "The Global Risks Report 2019, 14th Edition." World Economic Forum. Last modified 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
2. "Complexity In Cybersecurity Report 2019 - How Reducing Complexity Leads To Better Security Outcomes." Forrester Consulting and IBM. https://www.ibm.com/account/reg/us-en/signup?formid=urx-38409. May 2019.

A proactive cyber-defense is necessary to reduce the impact of security threats. This, however, does not eliminate the need for a reactive defense. A real-time, proactive defense augments the reactive defense to reduce the onslaught of attacks and attack vectors against the network.

Based on current industry research, there are four key drivers for the deployment of real-time security measures:

- Cyberattacks and security incidents remain prevalent and costly.
- Business operations cannot tolerate network or application downtime, especially when security attacks or component failures are the cause.
- Successful security monitoring depends on complete data visibility, including encrypted traffic.
- Control of solution costs and complexity depends on the amount of simplicity integrated into the solution.

Rampant and costly cyberattacks

The multitude of security breaches over the past several years has shown just how vulnerable organizations are to attack vectors in the wild. For instance, security breaches were up 11% from 2017 to 2018, according to a study by Accenture Security and the Ponemon Institute. This is a 67% increase in the last five years. The total cost of cybercrime for each organization also increased from $11.7 million USD in 2017 to $13.0 million in 2018. This is a rise of 12% in the last year and a 72% increase in the last five years.[3] Cybersecurity Ventures estimates that, by 2021, cybercrime is likely to cost the world $6 trillion per year, more than the combined gross domestic product of the UK and France.[4]

Malware is the most expensive attack type for most organizations. Cybersecurity Ventures predicts that global ransomware will cost $11.5 billion in 2019 and $20 billion in 2021 — 57 times the 2015 amount.[5] The Ponemon Institute found that the cost of malware attacks has increased by 11% from 2017 to 2018, and the cost of malicious insider attacks has increased by 15%.[6] Cybersecurity Ventures also predicts that a business will fall victim to a ransomware attack every 14 seconds by 2019, and every 11 seconds by 2021.[7]

3. Lasalle, Ryan M., and Paolo Dal Cin. "2019 Cost of Cybercrime Study | 9th Annual." Accenture | New Insights. Tangible Outcomes. New Applied Now. Last modified March 6, 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
4. Morgan, Steve. "2019 Official Annual Cybercrime Report." Herjavec Group. Last modified 2019. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
5. Morgan, Steve. "2019 Official Annual Cybercrime Report." Herjavec Group. Last modified 2019. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
6. Lasalle, Ryan M., and Paolo Dal Cin. "2019 Cost of Cybercrime Study | 9th Annual." Accenture | New Insights. Tangible Outcomes. New Applied Now. Last modified March 6, 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
7. Morgan, Steve. "2019 Official Annual Cybercrime Report." Herjavec Group. Last modified 2019. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Just as troublesome is the lack of ability to stop attacks. The Ponemon Institute found that 80% of cybersecurity and IT experts anticipate a "catastrophic" data breach at their companies by 2021 just from unsecure IoT endpoints.[8] In addition, a Microsoft study found that only 19% of businesses are highly confident in their organizations' ability to mitigate and respond to any type of cyber event.[9]

Fewer than half of IT respondents surveyed by LogRhythm indicated that their teams could detect a major cybersecurity incident within one hour. Most respondents who say it takes longer (more than two hours) to detect an incident are decision-makers. They also report that they do not have a security operations center (61%) or a formal program to protect against ransomware (64%), insider threats (68%), or denial-of-service attacks (71%).[10]

More importantly, the Ponemon Institute found that it takes organizations approximately 279 days to identify and contain a breach. This is the data breach life cycle. The 2019 data breach life cycle is 4.9% longer than the 266-day average in 2018. The longer a breach's life cycle is, the greater the total cost.[11]

An important number to know is the median length of time between intrusion and detection for incidents, which was 206 days in 2018, according to the Ponemon study.[12] The other 73 days in the 279-day lifecycle is the average time to contain the breach. Another unfortunate statistic is that 57% of breached companies must be informed of a security breach by someone else (law enforcement, partners, customers) – as they do not detect the breach themselves.[13]

8. Ponemon, Larry. "Ponemon Institute Announces the Release of the 2018 Megatrends Study." Ponemon Institute - Measuring Trust In Privacy And Security. Last modified March 15, 2018. https://www.ponemon.org/blog/ponemon-institute-announces-the-release-of-the-2018-megatrends-study
9. Microsoft. "By the Numbers: Global Cyber Risk Perception Survey." Marsh | Global Leader in Insurance Broking and Risk Management. Last modified February 2018. https://www.marsh.com/us/insights/research/global-cyber-risk-perception-survey.html
10. "2018 Cybersecurity Perceptions & Practices." LogRhythm, The Security Intelligence Company LogRhythm. Last modified 2018. https://logrhythm.com/cybersecurity-perceptions-practices-survey-white-paper
11. "2019 Cost of a Data Breach Report." Ponemon Institute and IBM. https://www.ibm.com/security/data-breach. 2019
12. "2019 Cost of a Data Breach Report." Ponemon Institute and IBM. https://www.ibm.com/security/data-breach. 2019
13. Trustwave. "2017 Trustwave Global Security Report." Trustwave. Last modified June 19, 2017. https://www.trustwave.com/en-us/resources/library/documents/2017-trustwave-global-security-report

Network and application downtime

Incident response is fraught with manual processes and bottlenecks. A recent report from Viavi Networks indicates that 83% of network teams are involved in resolving security issues.[14] Of those, 74% said they spend up to 10 hours per week, with another 17% saying they spend significantly more time.[15]

Adding to the ordeal for IT is that it often deploys security tools directly inline. This tactic creates a solid line of defense, but these tools also introduce points of failure in the network. Deployment of any tool on the live network carries the risk of becoming a single point of failure. Should the inline tool go down, it can take the network link it's on down with it.

While some security tools now include a bypass switch, that feature does not protect the network if IT has to take the tool offline for maintenance or upgrade. An EMA study found that one-third of enterprises schedule downtime for security appliance updates.

This approach usually happens overnight or on weekends, and the work must be completed within a specified window.[16] This adds to the frustration and stress.

Network visibility and decryption

IT security and analytics tools are only as good as the data they see. IT has more traffic to monitor, coming from more sources, and carrying more threats than ever before. Globalization, the Internet of Things, cloud, virtualization, and mobile devices are forcing companies to extend their network edge — often into places where they cannot easily gain visibility.

This causes blind spots, which like a dark alley, provide a place for attacks to go unnoticed. In fact, blind spots have become a serious security issue for enterprises and service providers. According to the 2017 Trustwave Global Security Report, most victimized companies do not discover security breaches themselves.[17]

14. VIAVI Solutions. "Wire Data Is Now The #1 Network Data Source for Security Incidents: Twelfth Annual "State of the Network" Survey from VIAVI." PR Newswire: Press Release Distribution, Targeting, Monitoring, and Marketing. Last modified July 16, 2019. https://www.prnewswire.com/news-releases/wire-data-is-now-the-1-network-data-source-for-security-incidents-twelfth-annual-state-of-the-network-survey-from-viavi-300885288.html
15. VIAVI Solutions. "Wire Data Is Now The #1 Network Data Source for Security Incidents: Twelfth Annual "State of the Network? Survey from VIAVI." VIAVI Solutions. Last modified July 16, 2019. https://www.viavisolutions.com/en-us/news-releases/wire-data-now-1-network-data-source-security-incidents-twelfth-annual-state-network-survey-viavi
16. McGillicuddy, Shamus. "Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics." Niagara Networks | Next Generation Network Visibility. Last modified August 2018.
17. Trustwave. "2017 Trustwave Global Security Report." Trustwave. Last modified June 19, 2017. https://www.trustwave.com/en-us/resources/library/documents/2017-trustwave-global-security-report

Threats obfuscated by encryption can bypass many security controls. Fifty-nine percent of businesses surveyed by Forrester Consulting report that getting visibility into security-related data and insights from across the organization is a top challenge.[18] The sudden and rapid expansion of a new or unknown application can enable threats to go undetected until they jeopardize the availability and health of the network.

The use of encryption for legitimate traffic and malicious cyberattacks alike continues to grow. In 2017, SonicWall reported that 68% of sessions used SSL/TLS encryption. By the end of 2018, that percentage had grown to 69.7%.[19]

According to Cisco Systems, "More than 70% of malware campaigns in 2020 will use some type of encryption to conceal malware delivery, command-and-control activity, or data exfiltration. And 60% of organizations will fail to decrypt HTTPS efficiently, missing critical encrypted threats."[20]

Security architecture complexity

Security environments are increasingly complex. In fact, the following data from a Forrester Consulting report shows that 91% of organizations are concerned about complexity in IT networks. Security professionals tend to operate in siloed teams, so it is rare — if not impossible — to get a full picture of data and processes across the entire security discipline. As an example, 72% believe simplification would have a "moderate" or "significant" improvement in operational efficiency, security staff productivity (68%), and security investment return (58%) — addressing their highest priorities.[21]

A study by Jon Oltsik, senior principal analyst at Enterprise Strategy Group (ESG) and the founder of the firm's cybersecurity service, uncovered similar findings. According to his research, "83% of respondents believe network security has become more complicated over the last two years." That research also showed that this complexity is a direct cause of security incidents at 29% of organizations.[22]

18. "Complexity In Cybersecurity Report 2019 - How Reducing Complexity Leads To Better Security Outcomes." Forrester Consulting and IBM. https://www.ibm.com/account/reg/us-en/signup?formid=urx-38409. May 2019.
19. "2018 Sonicwall Cyber Threat Report Threat Intelligence, Industry Analysis, and Cybersecurity Guidance for the Global Cyber Arms Race." Sonicwall. Last modified 2018. https://cdn.sonicwall.com/sonicwall.com/media/pdfs/resources/2018-snwl-cyber-threat-report.pdf
20. "Cisco Encrypted Traffic Analytics." Cisco. Last modified July 2019. https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf
21. "Complexity In Cybersecurity Report 2019 - How Reducing Complexity Leads To Better Security Outcomes." Forrester Consulting and IBM. https://www.ibm.com/account/reg/us-en/signup?formid=urx-38409. May 2019.
22. Oltsik, Jon. "Navigating Network Security Complexity." Enterprise Strategy Group. Last modified June 2019.

Organizations are spending more but not necessarily getting more security for their money. Increases in security budgets and organizational pressure to avoid a damaging data breach have led them to adopt a plethora of disconnected point solutions. On average, organizations have added 52% more security products and 77% more vendors over the last two years according to Forrester Consulting. In addition, they are managing an average of 25 different security products or services from 13 different vendors.[23]

Another study from LogRhythm showed that 95% of respondents use security software to prevent and react to threats. In fact, more than one-quarter of decision-makers deploy more than 10 security software solutions to manage security threats. Only about 40% use five or fewer.[24]

Jon Oltsik from Enterprise Strategy Group sums up the problem this way, "What's killing security is not technology; it is operations. Companies are looking for ways to reduce their overall operations requirements and need easy-to-use, high-performance solutions to help them do that."

In the end, system complexity increases the cost of a breach by $290,000, for an average cost of $4.21 million, as evidenced by a report from the Ponemon Institute.[25]

Solving the problem with inline security

Effective security monitoring depends on having visibility into traffic across all links in your network, including virtual and encrypted traffic, without the danger of dropped packets. The larger and more complex your network, the greater the probability of network blind spots and the risk of threats going undetected. That is why a strong visibility architecture should be the foundation of your security architecture. The tremendous amount of data that traverses your network needs quick inspection to identify packets that need further analysis.

One way to address risks mentioned above is to create an inline security architecture. This allows you to immediately inspect and stop bad traffic before it ever enters your production network. This is why Enterprise Management Associates state that 78% of enterprises have connected security technology to inline network packet brokers.[26]

23. "Complexity In Cybersecurity Report 2019 - How Reducing Complexity Leads To Better Security Outcomes." Forrester Consulting and IBM. https://www.ibm.com/account/reg/us-en/signup?formid=urx-38409. May 2019.
24. "2018 Cybersecurity: Perceptions & Practices." LogRhythm. Accessed September 12, 2019. https://www.jas-solution.com/document/LogRhythm/LogRhythm_Cybersecurity_Practices_and-Attitudes_Benchmark_Study_2018.pdf
25. Rathod, Lakshna. "Cost of a Data Breach: Ponemon Institute Report." Diligent. Last modified August 13, 2019. https://diligent.com/en-gb/blog/cost-of-a-data-breach-ponemon-institute-report
26. McGillicuddy, Shamus. "Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics." Niagara Networks | Next Generation Network Visibility. Last modified August 2018.

While an inline security architecture will not create a foolproof defense against all these threats, it provides the crucial data access security engineers need. Data is the life blood for any security architecture. The wrong data can result in false positives, even worse missing data can result in false negatives, leaving you feeling safe when in fact you are not.

Combining inline visibility with inline security appliances creates a formidable defense. For instance, extensive use of encryption, data loss prevention, threat intelligence sharing, and the integration of security into the software development process are all associated with lower-than-average data breach costs. Among these, encryption had the greatest impact, reducing breach costs by an average of $360,000, according to the Ponemon Institute.[27]

The following chart shows a summary of four security-related problems and the inline solution that can be deployed to mitigate, if not remedy, the issue.

Key Specifications	Options
Cyberattack prevalence and cost increasing	Reduce number and cost of breaches • Deploy inline tools to inspect data • Add an NPB to make data distribution easy
Network and application downtime	Increase network and application availability • Insert external bypass switches to support business continuity fail-overs • Use NPB for n+1 tool survivability • Deploy NPB in high-availability model
Lack of data visibility, including encrypted traffic	Insert a visibility architecture • Deploy an NPB to regenerate data to multiple tools for analysis • Deploy an NPB with internal SSL decryption • Deploy an external appliance to perform SSL decryption
Increasing amount of complexity	Replace complexity with simplicity • Use an NPB for remote access to tools • Use an NPB for simplified programming with a graphical user interface (GUI) • Use an NPB for serial tool chaining • Use an NPB for aggregation and filtering of data • Use an NPB for deduplication (if needed) to remove any extraneous data

Table 1. Potential solutions for the four most common security problems

27.Rathod, Lakshna. "Cost of a Data Breach: Ponemon Institute Report. "Diligent. Last modified August 13, 2019. https://diligent.com/en-gb/blog/cost-of-a-data-breach-ponemon-institute-report

The Inline Visibility Architecture

Inline means that a component or tool is deployed directly in the path of network data flow. This includes both security tools and network visibility equipment. In the case of visibility equipment, this would be a bypass switch, packet broker, and security appliances. One drawback to this approach is that if any system in the data path fails, the link goes down. Fortunately, there are solutions providing fail-over and redundancy that eliminate the failure concern.

External bypass switch

The purpose of a bypass switch is to switch traffic around tools that have either gone down due to some fault or issue with power or tools that need to be taken offline for software updates, patches and subsequent reboots.

You can set a bypass switch to fail open or fail closed. Fail open means that traffic continues to flow between network devices if you remove a security monitoring device from the network or the bypass switch loses power. This mechanism is also referred to as "fail to wire" to make it clear that this failure scenario supports business continuity, versus the fail-closed scenario, where failure in the bypass switch results in no traffic passing, the safest option.

The bypass switch generally uses a heartbeat packet to detect application, link, or power failure on the attached monitoring device. If the heartbeat packet is disrupted, then the bypass switch removes this point of failure by automatically shunting traffic around the security tool whenever the tool is incapable of passing traffic.

While directly deploying inline security tools can create a line of defense, these tools can also result in single points of failure. Even a strong mix of security and analytics tools can lead to network reliability risks as regular rebooting, maintenance, and upgrades of those tools increase the chances of a costly network outage. If an inline tool becomes unavailable, it can completely bring down the network link, significantly compromising network uptime and disrupting business continuity. This can be a significant problem for the almost 20% of IT organizations that directly deploy inline security tools and the 40% that deploy internal bypass solutions instead of external-based solutions.[28]

An external bypass switch allows fail-safe deployments of inline security and monitoring tools to ensure high availability and maximum uptime. The stand-alone (external) bypass offers superior protection when compared to a security tool with an integrated bypassoption.

28. McGillicuddy, Shamus. "On-Demand Webinar: Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics." Enterprise Management Associates. Accessed September 12, 2019. http://info.enterprisemanagement.com/next-gen-network-packet-brokers-webinar-ws

For example, some external bypass switches have a mean time between failure (MTBF) of approximately 450,000 hours. This reliability can be up to five times better than various security tools (such as combined firewall and IPS solutions) that have an MTBF of approximately 80,000 to 100,000 hours. Adding internal bypass capability further reduces the MTBF and reliability for those types of solutions.[29]

Also, when you replace various security tools, you may have to remove the integrated bypass as well. An external bypass eliminates this issue.

Another key benefit to the external bypass switch is fail-over capability during upgrades. Certain inline security tools include an internal bypass switch. This becomes a problem when you want to replace the security tool, or, in some cases, simply update and maintain that tool. Software upgrades or security patches may require a reboot, with obvious negative implications for architectures using internal bypass switching. The simple solution is to use an external bypass. Then you do not have to worry about future upgrades.

An external bypass offers the following benefits:

- It eliminates single points of failures for inline tool deployments with a bypass switch.
- The MTBF of an external bypass switch can be up to five times better than an integrated bypass.
- It provides more flexibility to add or remove inline security tools without network impacts.
- An external bypass switch eliminates downtime from tool upgrades and removal.

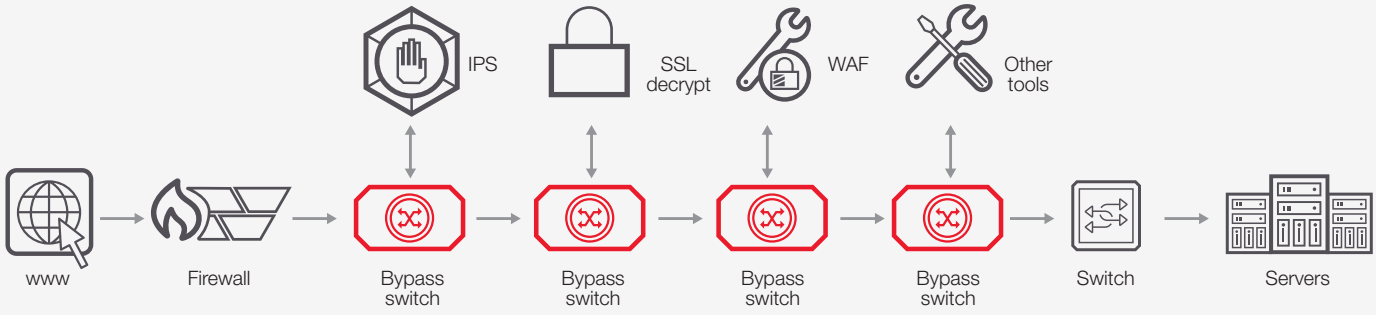

Figure 1. Inline security solution with a bypass switch connected to all components

29. Ixia conducted research

Inline network packet broker

The main purpose of the network packet broker is to optimize the flow of data going to security tools. Sitting between bypass switches and inline security appliances, packet brokers add another layer of data visibility to your security architecture. By providing the ability to aggregate, filter, deduplicate, load balance, and decrypt SSL / TLS traffic, packet brokers provide serialized data to a chain of security tools for deep data analysis.

Inline versions of NPBs also contain heartbeat and fail-over capabilities to properly handle data continuity and high-availability. This works similarly to the bypass switch, except that it is two-sided. There is communication between the bypass and NPB to make sure the NPB is working. If not, the bypass switch will either divert the flow into the network or stop the transmission of traffic completely. The exact action depends on the options selected for the bypass.

Another set of communications sits between the NPB and security appliances. This provides continuity and survivability for the data analysis process. Should a security appliance fail, the NPB will divert traffic to other available security appliances,

if available. If all security appliances are out of operational state, you can set the NPB configuration to operate in one of two ways. First, it could signal an error state to the bypass. The bypass switch will interpret this as a failure and follow its pre-programmed fail-open or fail-closed scenario. Once the security tools are operational again, the NPB replies to the bypass switch heartbeat message, and data flows from the bypass to the NPB again.

The second tool failure option is for the NPB not to declare an error and simply shunt the traffic back to the bypass. While this means that no security inspection takes place, the network remains up until one or more of the security tools becomes available again. Then the NPB will forward incoming traffic to the security tool(s).

The NPB supports load balancing. If one or more tools fail, the NPB will redirect to surviving tools. This is an excellent and cost-effective way of using n+1 survivability to create tool redundancy, assuming the tools are over-dimensioned by at least one device. The chapter on use cases provides more information on this functionality.

Another benefit from a packet broker is that you can automate the data inspection process. Tool chaining accomplishes this. Preset toolchains ensure that data is passed sequentially from one tool to another so that actions occur in sequences and do not get overlooked. Linking of security and monitoring tools happens by using software provisioning in the NPB to control the flow of data through the selected services. Depending on the situation, the required data inspection can occur in parallel or in series.

At Ixia, the primary way that we address tool chaining is to use a grouping of ports. To accomplish the proper flow of data, at least one tool gets assigned to a port or port group on the NPB. Multiple port groups require chaining together to accomplish the desired data flow.

The primary benefits of a packet broker are that it can help you with the following:

- improved uptime
- the ability to make real-time decisions
- extensive fail-over options
- cost savings resulting from load balancing across multiple tools
- built-in recovery options
- reduced complexity
- diversion of bad traffic to a honeypot

Complete visibility architecture diagram

The following diagram shows the proper way to integrate a bypass and an inline NPB into an inline security architecture.

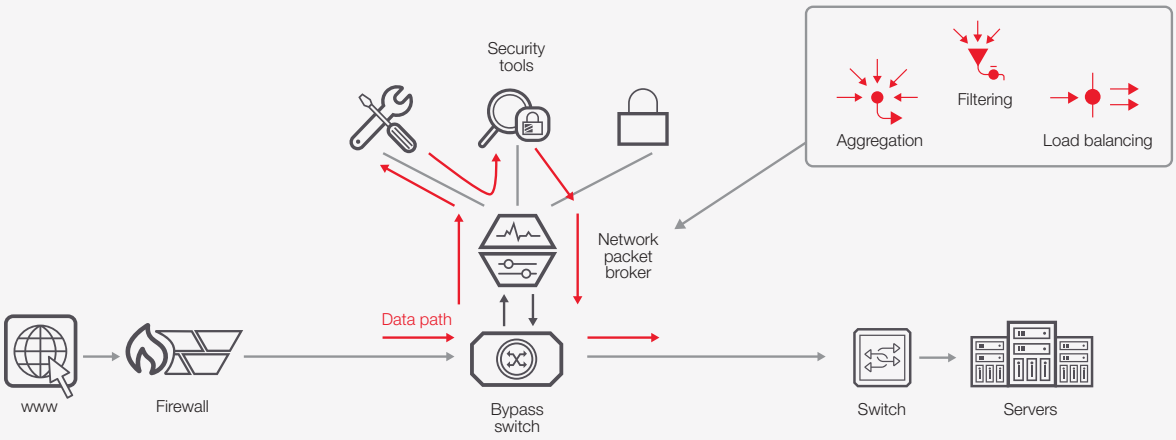

Figure 2. Inline security solution showing a typical traffic data path

Conclusion

Inline security solutions are a requirement for today's security architectures. Organizations cannot afford to ignore this type of solution anymore. The volume of security attacks, increasing network complexity, and the rapid growth in breach costs and risk is necessitating a change.

An inline solution starts with an external bypass switch and a network packet broker (NPB). Such a solution enables security teams to:

- increase network reliability with better fail-over
- improve security appliance survivability
- perform Secure Sockets Layer (SSL) decryption to expose hidden security threats
- reduce security architectural complexity
- better capture indicators of compromise (IOC)

Ixia can help you enhance your inline security deployments with a wide range of bypass switches and network packet brokers.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES