THE DEFINITIVE GUIDE

To Visibility Use Cases

ixia
A Keysight Business

CONTENTS

IMPROVE TROUBLESHOOTING AND NETWORK RELIABILITY

REMOVE NETWORK BLIND SPOTS

OPTIMIZE NETWORK PERFORMANCE

STRENGTHEN REGULATORY COMPLIANCE INITIATIVES

EXECUTIVE SUMMARY

Network visibility is an important topic. Most enterprises have hidden network and application problems. By exposing these problems, you can eliminate blind spots, improve efficiency, reduce costs, and optimize your troubleshooting efforts. The question is, how do you actually go about realizing these benefits? Success is based upon the solution(s) you choose to implement and how well you implement them. This book provides a collection of the top 68 network visibility use cases, along with a brief overview of how to implement each one. These summaries allow you to determine which use cases are critical for your business.

AN OVERVIEW OF NETWORK VISIBILITY

The source of many network problems is network visibility, or actually the lack of it. Lack of visibility is caused by blind spots – areas where you do not actually see everything that is happening. These blind spots exist in almost every network. It is not a question of "if" you have them, but where are they located.

Blind spots result from many sources including the following:

- The organizational structure of the business
- Technology complexity
- The monitoring and network equipment itself

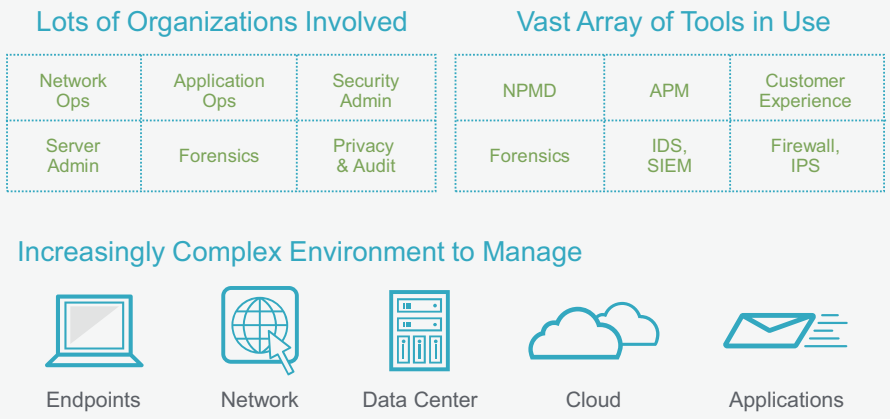


Figure 1 - The Modern Enterprise

While there are many examples of blind spots, here are some of the most common:

- Department silos
- Virtualization technology
- Rogue IT
- SPAN port usage
- New equipment
- Network complexity

If you want more information on blind spots, read this blog posted on the Ixia website.[1] It reviews 16 different types of blind spots and their sources.

So, what is the solution? It is something called a visibility architecture. A visibility architecture is simply a way to step back and take a look at your network, organize your network monitoring strategy, and then integrate that strategy with other strategies—like network security and troubleshooting.

By creating a visibility architecture, and it is a fairly simple task, you get a better understanding of what tools you have, where they access the network, and what data feeds into them. From there, you can optimize your monitoring strategy by pooling resources, load balancing data across tools, filtering out non-pertinent data to the tools, and integrating tools and data flows to eliminate problems faster than before. There are actual examples of businesses reducing their mean time to repair by up to 80%, just by creating a visibility architecture.

There are three basic components to a visibility architecture—the access layer, the control layer, and the traditional monitoring tool layer. In the past, people have typically said that the monitoring tools ARE the strategy, and so they did not need to plan anything else out. As a consequence, most enterprises have a mixture of all sorts of tools, many they do not even use, adding a lot of unnecessary complexity, and then, they still have a lot of network problems. Basically, the problems never magically disappeared. This is where a visibility architecture really helps.

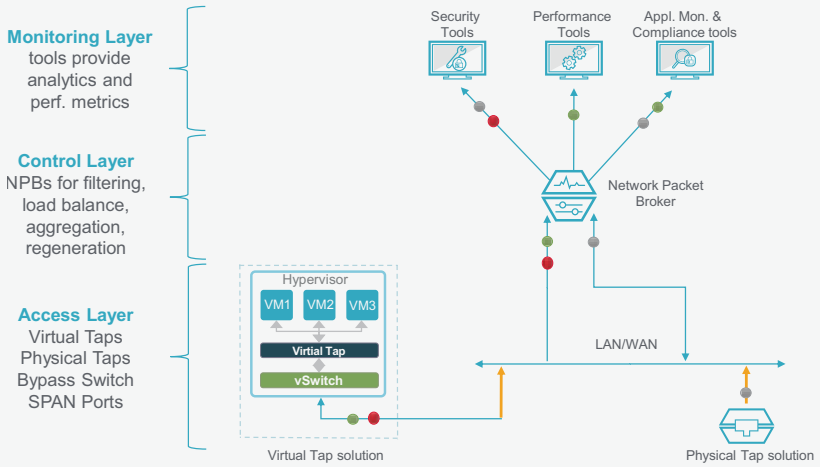


Figure 2 - Basic Illustration of a Visibility Architecture

The first layer of the model is the monitoring data access layer. This is provided by some sort of network access device, whether it's a physical tap, virtual tap, or mirrored port. In case you are not completely familiar with taps and what they are, a traditional tap is a piece of hardware that you insert into the network. It makes a copy of all the packets, whether they are good or bad. This copy can then be sent to monitoring equipment to be processed. Once the tap is inserted into the network, it's essentially set and forget. You normally do not have to do any programming to it. Taps are used for "out-of-band monitoring" because the monitoring equipment is not directly in the flow of network traffic. The tap is, but after that, all equipment that is receiving a copy of the traffic is completely out of the traffic path for network traffic. You can connect or disconnect whatever equipment you want to the tap monitoring port and it will NOT affect the rest of the network.

A second type of network access is a virtual tap, which is a software version of the hardware tap that you can use for VMware, KVM, Hyper-V, and cloud environments. The virtual tap allows you to export monitoring data outside of the virtual environment to security and monitoring tools in the physical data center.

The third type of network access is called a bypass switch. Think of this as a special tap for monitoring tools that you insert directly into the flow of the network data. If you had just inserted the tool, and it failed completely or you yanked the tool out, this would directly affect, i.e. stop the flow of data to the rest of the network. That is why we call it inline. Once a bypass tap is installed, connecting tools and monitoring equipment becomes more of a non-issue. The bypass tap adds in fail-over protection so that network disruptions are minimized to milliseconds. This way, if the tool has a problem (or if you want to change tools out), the bypass functionality can be engaged so that the bypass switch continues to pass all traffic directly downstream. Heartbeat signaling between the bypass switch and tools ensures automatic fail-overs for tool failures. This provides maximum network uptime.

A fourth type of access is called a Switched Port Analyzer (SPAN) port, also called a mirroring port, off of a network switch. While they make a mirrored copy of data, there are lots of issues with them. For example, they require programming, they have security issues, and they only provide summarized data, not a complete copy of all the packets. In fact, SPAN ports themselves are one of the reasons you can develop network blind spots. Again, check out the blind spot blog referenced earlier if you want more information on SPAN ports.

The next layer uses a network packet broker, also called an NPB, which allows you to filter, aggregate and load balance data. From a business point of view, there are several high-level benefits that packet brokers provide. This includes connectivity, reduced tool costs, scaling, reliability, and longevity.

Packet brokers are designed to augment your monitoring tools, not replace them. In essence, they are a low-cost way to help turbo charge the efficiency and capabilities of your monitoring tools. There are different sizes and capabilities associated with different packet brokers. All packet brokers should perform filtering, load balancing, aggregation, and advanced features (like deduplication) for Layer 2 through 4 data. Some also provide application layer features like (application filtering, NetFlow generation, Secure Sockets Layer (SSL) decryption, data masking, etc.). The exact feature set depends upon your needs.

There are also packet brokers that offer specialized functions for inline or out-of-band deployments. For instance, an inline packet broker (that is inserted between a bypass switch and inline security tool) can offer capabilities like high availability (HA) for mission critical deployments, the serial chaining of security tools, load balancing of data to inline tools, and filtering of inline data to improve the efficiency of intrusion prevention system (IPS) and other tools. Out-of-band solutions can help you optimize your out-of-band tool deployments and control your costs.

After the packet brokers are the monitoring tools. This is probably what most people are familiar with. Instead of receiving the data directly from a tap, these tools now receive filtered data that is more relevant and concise. This makes the tools more efficient.

If you want more details on these areas, check out the Visibility Architecture solution page on the Ixia website.[2]

Let us look at packet brokers a little closer. With a network tap, you get a complete copy of ALL of the raw data you intend to send to your tools. Unfortunately, from the tool perspective this is like drinking from a street-level water main. There is a lot of data that can quickly overwhelm the monitoring tools. And, your tools are limited to the fixed number of ingress ports provided on the device.

With a network packet broker we introduce filtering. Basic packet brokers can do Layer 2 through 4 filtering and load balancing. This means we can filter on the source and destination Internet Protocol (IP) address, port numbers, virtual local area networks (VLANs), etc., which minimizes the amount of traffic going to each monitoring tool. This is an improvement as it makes more efficient use of tool capacity and makes it easier to scale tools as needed. But this is still akin to drinking from a fire hydrant now for the tools—the volume is less than before, but it is still too much.

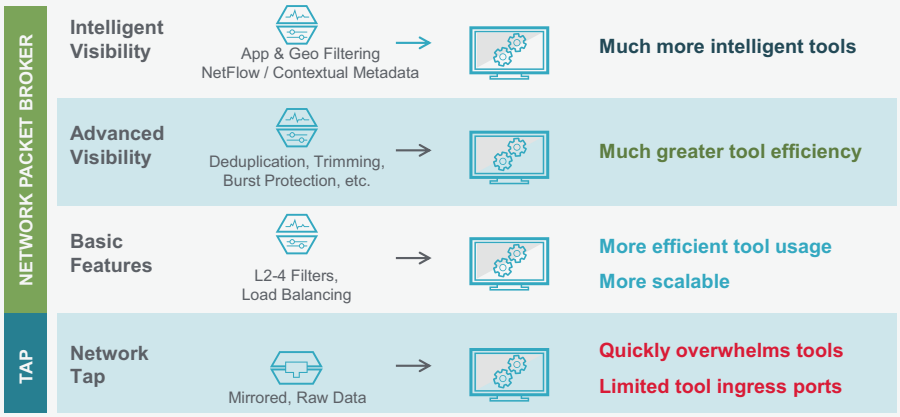


Figure 3 - Basic Illustration of the Benefit of Data Filtration

Advanced packet brokers can perform even more functions. Most notably, they can do deduplication of traffic to minimize the traffic a tool must process. They also provide packet trimming to remove the packet payload, if it is not needed. And they can do protocol stripping, so tools can analyze encapsulated traffic like GPRS Tunneling Protocol (GTP), Multiprotocol Label Switching (MPLS) and other tunneling protocols. Some even have deep buffering to provide burst protection for tools that operate at lower speeds. This greatly reduces the traffic that the tools need to analyze. All of which makes the monitoring solution MUCH more efficient. Now the flow of data is figuratively the size of the water pipe going into your house and the tool can spend its maximum central processing unit (CPU) capability processing relevant data, not on functions like deduplication.

Finally, some manufacturers also provide a more advanced level of intelligence for packet brokers. What this means is that these packet brokers are able to perform application intelligence, which lets the packet broker do true signature-based application identification and filtering along with the correlation of metadata information like geolocation, user device type, and user browser type. This gives you much more control over exactly what you want to monitor.

If your tools can not consume packet-level data, the packet broker can generate NetFlow metadata. But some go beyond simple NetFlow and provide additional metadata that gives your tools very detailed contextual information. Now, the figurative flow of data is the size of a garden hose. You have the right amount of data going to the right tools. What this really means is that your monitoring tools can now be much more intelligent, not just more efficient. The tools have access to data and intelligence in a way not possible with other visibility solutions.

Another item to consider is what type of deployment scenario you will be using for your visibility solutions. The most common scenario, mentioned earlier, is an out-of-band visibility solution. Figure 4 provides a basic illustration. As you can see, the packet broker and tools are not in the flow of network traffic. The tap is, but nothing else is.

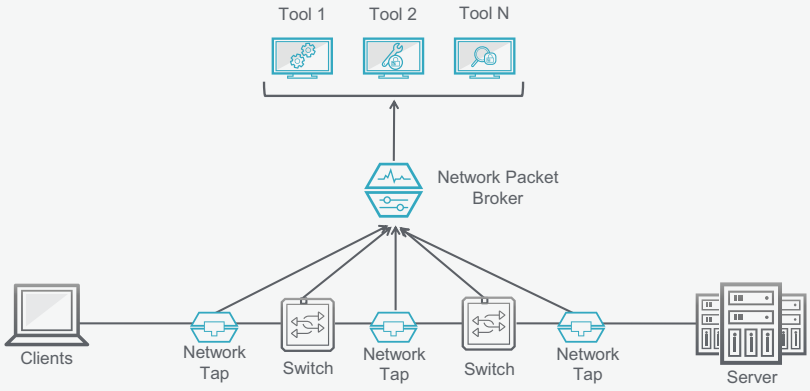


Figure 4 - Basic Example of Out-of-Band Network Visibility

The previous diagram was a basic one. Figure 5 shows the out-of-band solution in more detail.

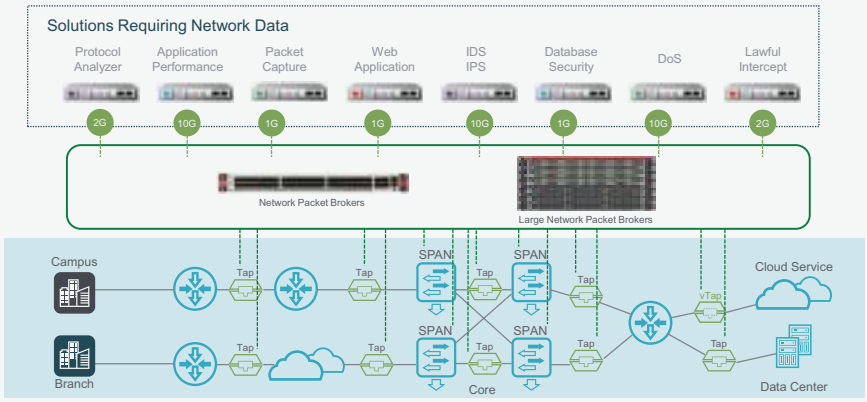


Figure 5 - Detailed Example of Out-of-Band Network Visibility

Monitoring data will come in from many network locations and sources. This affects the size of the packet broker needed because it then feeds 5, 10, 15, maybe 20 or more different security and monitoring tools that have different requirements like:

- They need unencrypted data
- They can only handle certain data rates, like 10 Gbps or 40 Gbps
- They only want to see specific data content

A second visibility solution is what we commonly refer to as inline visibility. Simply put, this means that the tap (which is actually a bypass switch) and the packet broker are DIRECTLY in the path of the data flow. If either of these components fail, the flow of data stops. Fortunately, solutions like the one from Ixia have fail-over and redundancy options that eliminate the failure concern.

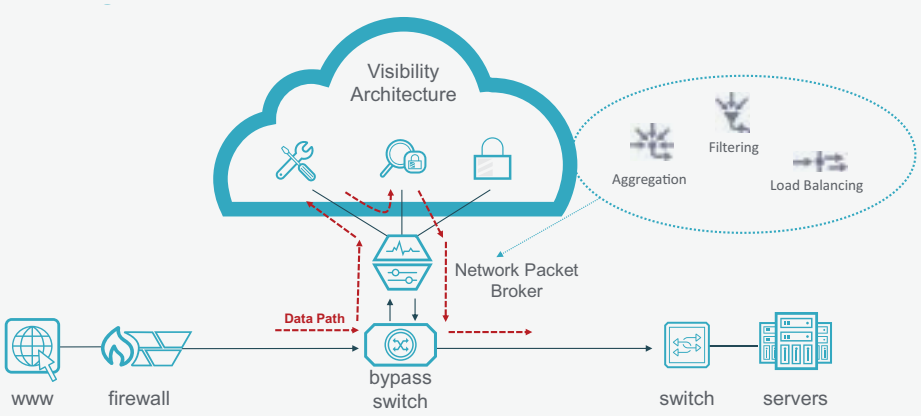


Figure 6 - Basic Example of Inline Network Visibility

SUMMARY OF NETWORK VISIBILITY USE CASES

So now that you know what network visibility is, what can you really do with it? There are lots of value-added use cases, literally 67 different use cases for network visibility, that you can deploy. They can generally be organized into the six categories of fundamental benefits that you see here:

- Improving network security
- Providing cost containment and cost reduction capabilities
- Speeding up troubleshooting efforts and improving network reliability
- Removing network blind spots
- Optimizing network performance
- Strengthening regulatory compliance initiatives

These six areas are where the rubber meets the road. It is not expected that all 67 of the solution sets will apply to everyone, but you should be able to find at least 1, if not 2 to 5, that WILL be useful to you. One note here, we have grouped the various out-of-band and inline solutions according to the six different categories. So, the solution sets, as presented here, are not intended to build upon one or another. They are all independent of each other. This approach allows you to focus on the solution itself and illustrate how the solutions might be of use, rather than focusing on installed equipment, rollout plans, prerequisites, etc. needed for the different solutions.

Here is a quick summary of the 68 most common solutions, by category:

NETWORK SECURITY IMPROVEMENTS

1. Data Filtering for Rapid Forensic Investigation Limits Breach Damage
2. Improve Network Reliability With External Bypass Switches
3. Application Intelligence Captures Indicators of Compromise
4. Out-of-Band Data Filtering Improves Security Tool Efficiency
5. High Availability Makes Inline Security Tool Deployments More Reliable
6. N+1 Redundancy Delivers Reliability at a Fraction of the Cost of HA
7. Easily Enable Appliance-Based SSL Inline Decryption with an NPB
8. Simplify Inline SSL Decryption Using an NPB with Integrated Decryption
9. Threat Intelligence Gateways Reduce False Positive Security Alerts
10. Serial Tool Chaining of Data Improves the Data Inspection Process
11. Self-Healing Inline Security Architectures Maximize Network Availability
12. Protect Your Network with an NPB and a Honeypot
13. Save Time and Money when Deploying ASA Firewall Migrations
14. SIEM Integrations Automate Threat Detection and Mitigation

DELIVER COST CONTAINMENT AND EFFICIENCY INCREASES

15. NPB-Based Data Filtering Allows Monitoring Tools to Scale Efficiently
16. Deduplication Increases Monitoring Tool Efficiency and Accuracy
17. Load Balancing Extends the Life of 1/10 Gbps Tools in 40 Gbps Networks
18. Maximize Monitoring Tool Efficiencies with Data Aggregation
19. Eliminate SPAN Port Contention Issues
20. Increase Tool Efficiency by Combining Virtual and Physical Monitoring
21. Track Your Monitoring Data to Optimize Network Performance
22. Optimize Network Traffic with Cisco Nexus 3000/9000 Integration
23. Header Stripping Increases Efficiency of Monitoring Tools
24. Protect Monitoring Data with Extended Burst Protection
25. NPB Automation Dramatically Improves Monitoring Response Times
26. Reduce TCO with Effective Visibility Architecture Management
27. Lower Your OPEX by Integrating Monitoring and Network Management
28. Validate Latency for High Performance Financial Monitoring Links

SPEED UP TROUBLESHOOTING EFFORTS AND IMPROVE NETWORK RELIABILITY

29. Reduce/Eliminate the Need for Change Board Approvals and Crash Carts
30. Floating Filters Dramatically Cut Data Collection Times
31. Dynamic Filter Engines Increase Data Filter Accuracy
32. Improve Out-of-Band Monitoring Solution Reliability with HA
33. Conduct Proactive Troubleshooting with Application Intelligence
34. Baseline Your Network to Recognize Aberrant Behavior
35. Improve Troubleshooting with Quick Packet Captures
36. Use Duplicate Packets to Isolate Architecture Design Flaws

37. Easily Validate Your Monitoring Filter Accuracy
38. Improve Network Reliability Analysis with Better Monitoring Data
39. Correlate Production Traffic with Test Environments

REMOVE NETWORK BLIND SPOTS

40. Visibility Architectures Expose Missing/Hidden Data
41. Tap Deployments Improve Data Collection
42. Virtual Taps Expose Hidden East-West Traffic in Virtual Data Centers
43. Regenerate Monitoring Data for Distribution to Multiple Destinations
44. Acquire Visibility into Cloud Networks
45. Eliminate Data Overloading of Network Switch SPAN Ports
46. Reduce Network Complexity with Visibility Architectures
47. Monitor Cisco ACI Switching and Mirroring Solutions with Ease
48. Overcome Visibility Loss Due to M&A Network Integrations
49. Improve Sandboxing Exercises to Validate Network Designs

OPTIMIZE NETWORK PERFORMANCE

50. Application Intelligence Identifies Slow or Underperforming Applications
51. Application Performance Monitoring Delivers Network Optimization
52. Proactive Monitoring Creates Better and Faster Network Rollouts
53. Optimize Network Performance Monitoring Effectiveness
54. Prevent Application Bandwidth Overloads on Your Network
55. Use a GTP Session Controller to Improve Carrier Customer QoE
56. Improve and Simplify Voice Quality Monitoring Efforts
57. Focused Deep Packet Inspection Optimizes Your Network Data
58. Conduct Inline Network Performance Monitoring
59. Better Data Collection Makes QoE Monitoring More Effective
60. Offload NetFlow Data Generation to Improve Switch Performance

STRENGTHEN REGULATORY COMPLIANCE INITIATIVES

61. Enhance Regulatory Compliance with Data Masking
62. Discover Rogue IT on Your Network
63. Search for and Capture Specific Data with Application Intelligence
64. Packet Trimming Eliminates Sensitive Data Propagation
65. Perform Lawful Intercept Data Captures
66. Enforce IT Network Security and Compliance Policies Enforce IT Network Security and Compliance Policies
67. Document Security Policies for Regulatory Compliance

Network Security Improvements

THESE SOLUTIONS PROVIDE EXAMPLES OF HOW TO DETECT AND MINIMIZE SECURITY THREATS

ixia
A Keysight Business

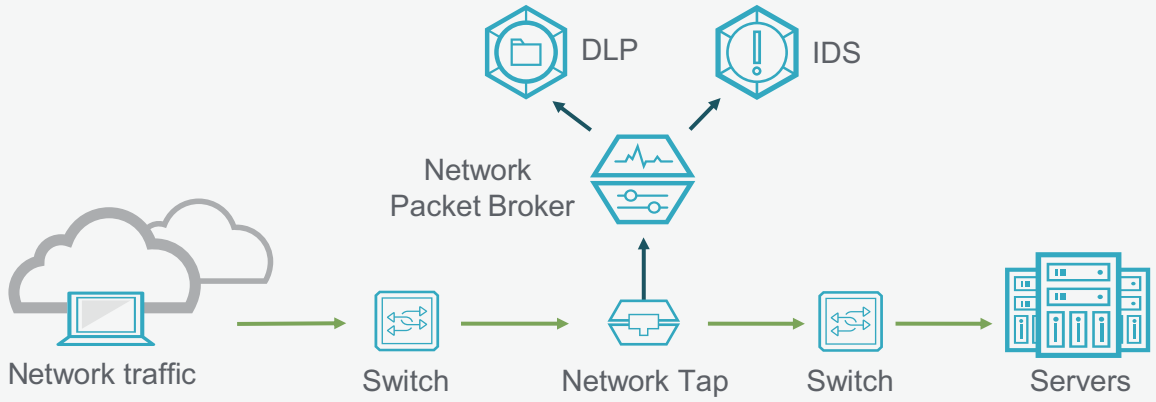
915-8138-01-9081 Rev B

1 - DATA FILTERING FOR RAPID FORENSIC INVESTIGATION LIMITS BREACH DAMAGE

SOLUTION SUMMARY

- In 2016, only 43% of breaches were self-detected[3]
- Create NPB filters to collect L2 through L4 data and send it to DLP, IDS, log file tools, and other security tools for analysis
- Perform forensic analysis to see data exfiltration attempts and limit data loss

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

According to the 2017 Trustwave Global Security Report, 43% of breaches are self-detected.[3] While this number is up from previous years, it means that 57% of breaches are still detected by someone else. Law enforcement, suppliers, or customers had to notify the victimized company that it had been breached because they did not know themselves.

To be effective at stopping and detecting as many network security threats as possible, you need an integrated security and visibility architecture. Just purchasing security tools is not an effective approach. Taps and an NPB can be used to 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 intrusion detection system (IDS), for analysis.

Well-designed NPBs allow information technology (IT) engineers to selectively screen 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. The DLP(s) are used to extensively review suspect data, analyze it to make a determination, and then pass that information on to other devices.

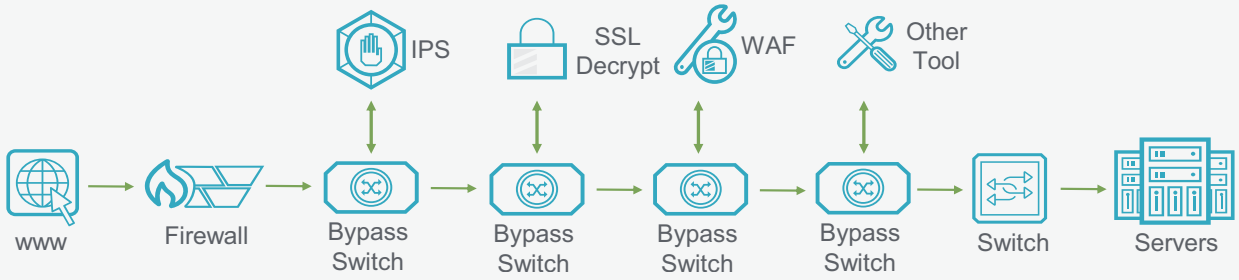
NetFlow data can also be delivered to security and analysis tools, like a security information and event management (SIEM), for analysis and security decisions. The SIEM could have the information quarantined, or it could be delivered to a storage device so that an IT engineer can review the data as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

2 - IMPROVE NETWORK UPTIME WITH EXTERNAL BYPASS SWITCHES

SOLUTION SUMMARY

- Eliminate single points of failures for inline tool deployments with a bypass switch
- The MTBF of an external bypass switch can be five times better than an integrated bypass[4]
- More flexibility to add/remove inline security tools without network impacts
- External bypass switches eliminate downtime because of tool upgrades/removal

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

An external bypass switch allows failsafe deployments of inline security and monitoring tools to ensure high availability and maximum uptime. The purpose of a bypass switch is to eliminate the pain of direct deployments of inline tools. 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 will increase the chances of a costly network outage. In the event that 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 enterprises that directly deploy inline security tools and the 40% that deploy internal bypass solutions instead of external-based solutions.[5]

Bypass switches fit into the existing networking ecosystem allowing the existing network to function as currently designed without forcing changes to accommodate network visibility components. However, bypass switches give you more flexibility to add/remove inline security tools without network impact. When the fail-open bypass function is activated, all traffic can continue downstream. The failover time is typically less than 10 milliseconds. If you prefer a fail-closed option (where no traffic continues in or out of the network), that is available as well. Typical failures are indicated by Link Fault Detection (LFD). However, a self-healing architecture using heartbeat messages (that are passed back and forth between the bypass and NPB/tools to ensure network availability) can be used as well.

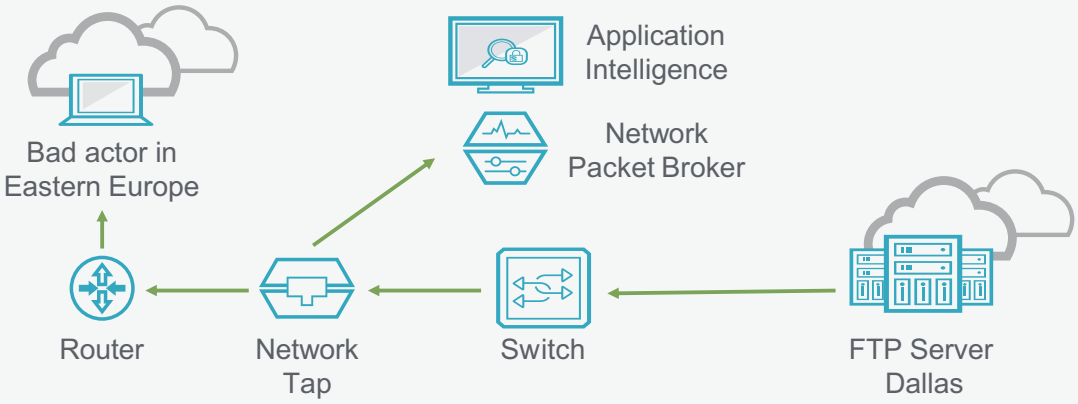
The stand-alone (external) bypass offers superior protection when compared to a security tool with an integrated bypass option. For example, some external bypass switches have been shown to have a mean time between failure (MTBF) of approximately 450,000 hours. This reliability can be up to 5 times better than various security tools (like combined firewall and IPS solutions) that have an MTBF of approximately 80,000 to 100,000 hours.[5] Adding internal bypass capability further reduces the MTBF and reliability for those types of solutions. In addition, when you replace various security tools, the integrated bypass may have to be removed as well, destroying any supposed bypass advantage. An external bypass eliminates this issue.

3 - APPLICATION INTELLIGENCE CAPTURES INDICATORS OF COMPROMISE

SOLUTION SUMMARY

- 68% of breaches happen over the course of days[6]
- Create an NPB filter to collect detailed user geolocation, data transfer sizes, etc.
- See data exfiltration attempts in real-time and stop them

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Application intelligence can be used to help improve network security by exposing indicators of compromise. Packet brokers can perform filtering and other functions for application data, flow data, and metadata to provide a higher level of intelligence within your visibility architecture. This intelligence provides actionable insight that you can use to see macroscopic trends and indications of issues across your network. Consider this; according to the 2016 Verizon Data Breach Investigations Report (DBIR) report, almost 68% of breaches happen over the course of several days.[6] A rapid response to security threats can help minimize the cost of a breach based upon this information. Unfortunately, this is not the norm. According to the 2016 Trustwave Global Security Report, the average time for breach detection was 168 days.[7] This gives the intruder plenty of time to exfiltrate any data they want. What if you could reduce the 168 days to 168 seconds or something like that? This use case is one example of how to do it.

One example is a bad actor over in Eastern Europe performing unauthorized data exfiltration. The bad actor gets into your network and starts transferring files from a server in Dallas. Application intelligence, or at least the Ixia version of it, can combine application information, bandwidth information, and geolocation information to show that someone in Eastern Europe has accessed a server in Dallas using file transfer protocol (FTP) and is transferring that data to a location back in Eastern Europe.

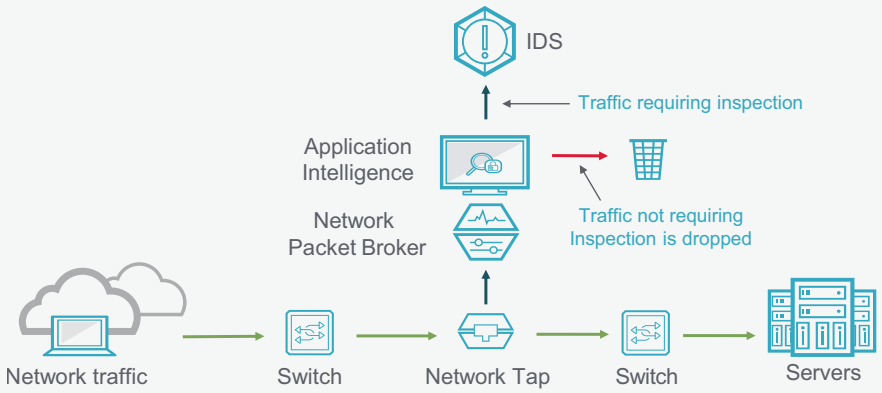
Is this a problem? Well, that depends upon whether you have any authorized users in Eastern Europe or not. If not, you should consider investigating this as soon as possible. In any case, you have the information right in front of you, it is up to you what you do with it. And it does not take a 168 days to discover this. It is actually much closer to the 168 seconds. This is just one example of how application intelligence can expose indicators of compromise.

4 - OUT-OF-BAND DATA FILTERING IMPROVES SECURITY TOOL EFFICIENCY

SOLUTION SUMMARY:

- Business IP traffic will grow by a factor of nearly 3 between 2016 and 2021[8]
- Not all data is of interest for security analysis. Use application intelligence to capture the right type of data and optimize data capture and filtering strategies.
- Application intelligence can improve the efficiency of certain tools up to 35%[9]

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Analyzing all of your network data costs a lot of money and the amount of data on your network will triple between 2016 and 2021.[8] You will need an extensive number of security tools and an extensive amount of your time to sift through the results. A better, more cost-effective approach is to isolate data that has a higher probability of being a security threat and analyzing just that data. This allows you to cost-effectively scale your security solution. An NPB with application intelligence can provide the capabilities necessary to perform this task.

This is 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 and can direct data to security tools based upon basic parameters. When Layer 7 data is used, contextual information based upon application type and routing information can be used to provide another layer of screening.

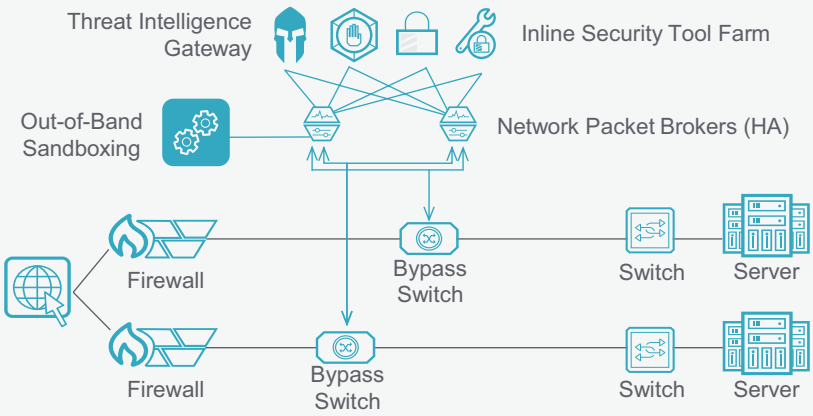
For instance, suppose that you are a university that has an extensive amount of data flowing across your network for research file transfers, communications (voice and email), and video (video conferencing, as well as streaming apps for students living on campus). Screening all of this data would take a long time and a lot of security tools. At the same time, some voice information (like voice over IP (VoIP) and Pandora) and some 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 still needs inspection can be routed on to an IDS for inspection. Employing this approach can reduce the amount traffic sent to an IDS by up to 35%, providing significant cost savings to the university IT staff.[10] They have literally cut their IDS tool costs by one-third.

5 - HIGH AVAILABILITY MAKES INLINE SECURITY TOOL DEPLOYMENTS MORE RELIABLE

SOLUTION SUMMARY

- The average cost of network downtime is $7,790 per minute[10]
- Use HA to create full redundancy (n+n) for inline deployments of NPBs and bypass switches
- Heartbeats enable super-fast fail-over between bypasses and NPBs

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

This solution is an illustration of how you can increase network reliability and security by implementing survivability. There are two common options—full redundancy (typically with a primary and standby set of tools connected) and then what is commonly called an n+1 option (where you have all of the tools connected and functioning with extra capacity). High Availability NPBs could be deployed for out-of-band tool deployments as well.

For the full redundancy option, this is highly effective at maintaining maximum network and tool up time. You literally have a second copy of every component (bypass switch, packet broker, and tools) in the network. If one component, or path fails, the secondary equipment can handle the load. While this option yields the highest level of MTBF, it also comes at a high price—literally doubling the cost for everything.

By using redundant external bypass switches and packet brokers, versus just redundant tools, you can increase your network uptime and reliability far beyond the level provided with just redundant tools. In addition, the external bypass switch and packet broker can reliably connect the redundant tools in a more cost effective and less complicated manner than special purpose load balancing devices. An external bypass approach has the benefits of delivering superior resilience due to more granular failure detection, faster failover, and better application session integrity. This reduces the cost of the system while making it more resilient at the same time.

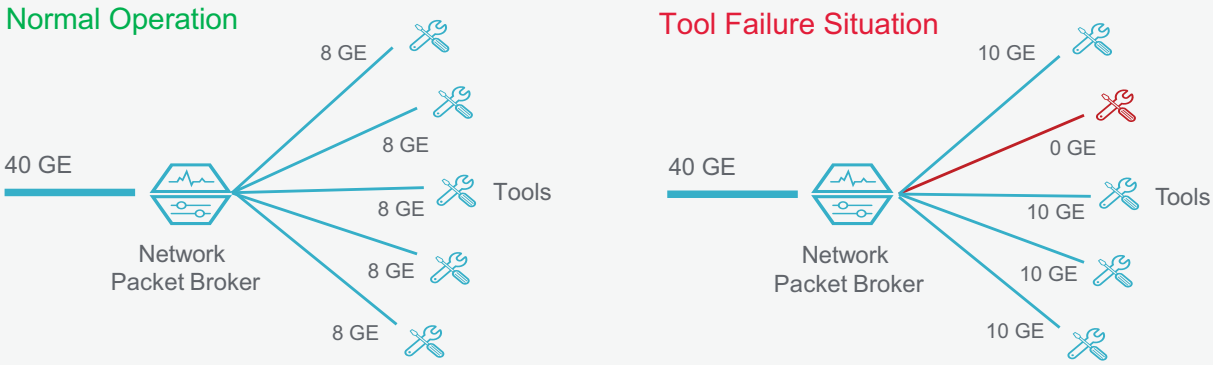
By deploying a redundant bypass switch and packet broker, you may not need a redundant set of tools. You could rely on the other equipment to provide the reliability. This option could then save you a lot of money, since security tools can be expensive.

6 - N+1 REDUNDANCY DELIVERS RELIABILITY AT A FRACTION OF THE COST OF HA

SOLUTION SUMMARY

- Deploy survivability to decrease risk and increase network security
- Inline deployments of NPBs and bypass switches using load balancing can create an n+1 survivability option
- Much more cost effective solution than HA but still delivers high reliability

Deployment scenario: Inline and out-of-band visibility architecture



SOLUTION OVERVIEW

Network security and monitoring tool survivability is often thought about in terms of redundant tools, especially in the case of inline deployments. However, an option to high availability is to implement an n+1 option for component redundancy. In this situation, you do not have a duplicate copy of tools waiting in a standby mode to take over should the primary equipment fail. At the same time, you do not have to spend double the costs for a redundant solution like you do with HA. Until now, cost has been identified as a significant contributor to the limiting of n+1 survivability.[11]

In this solution, security and monitoring tools are allocated to a specific port group on a network packet broker. Based upon filtering criteria, data traffic is then spread evenly across the port group. Should a heartbeat message (for inline solutions) or a Link Failure message (for out-of-band) solutions be received, the data is spread out across the remaining tools in the port group by the packet broker. Once the failed tool becomes available again, the NPB will resume routing traffic to it.

For example, let's say you need four IPS tools to process your inline network traffic. In this case, you would add a fifth IPS. The packet broker would then load balance the traffic across all five IPS tools. Should any one of the tools fail, the packet broker can load balance the full load across any of the remaining four IPSs. This provides a good level of survivability at a fraction of the cost of a fully redundant system.

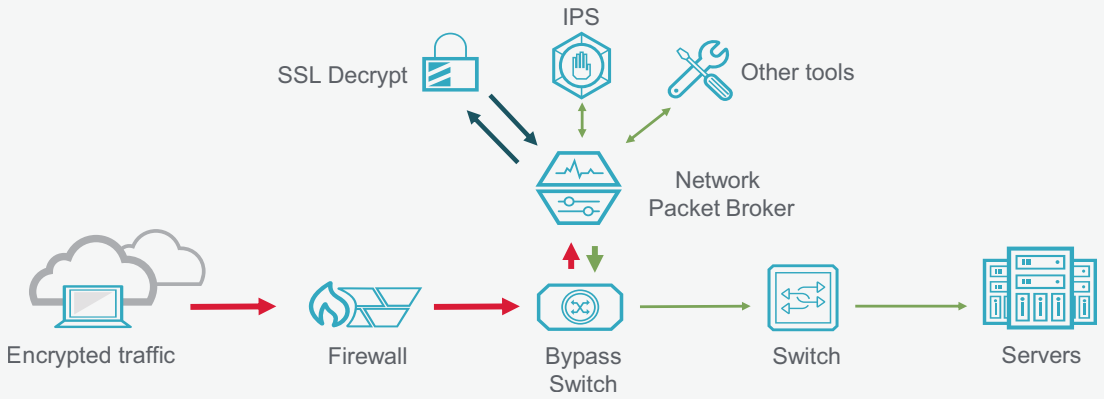
If you would like to have more survivability, like an n+2 situation, you can do that as well—all the way up to a fully redundant set of tools. It just depends upon the level of risk you feel comfortable with and your budget.

7 - EASILY ENABLE APPLIANCE-BASED SSL INLINE DECRYPTION WITH AN NPB

SOLUTION SUMMARY

- Up to 50% of all network security attacks in 2017 will use encrypted traffic to bypass security controls[12]
- Expose hidden threats with active decryption technology like A10 and Bluecoat
- NPBs allow for distribution of encrypted data to decryption devices and then the distribution of the now unencrypted data to various tools (NGFW, IPS, DLP, etc.)

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

Secure Socket Layer (SSL) and Transport Layer Security (TLS) encryption are standards-based technology for transmitting private information by protecting data packets from being read or corrupted by non-authorized users. They use a combination of public-key and symmetric-key encryption to create an encrypted link between a server (typically a website or mail server) and a client (typically a browser or a mail client). For most organizations, SSL traffic is already a significant proportion of their total Web traffic. Many vertical market segments are subject to rigorous compliance protocols that actively demand SSL encryption, such as Payment Card Industry Data Security Standard (PCI-DSS) and Health Insurance Portability and Accountability Act of 1996 (HIPAA). Such regulations aim to protect sensitive data in transit travelling to banking, merchant, and healthcare-related websites.

Direct tangible threats within SSL encrypted traffic include malicious code disguised by the encryption process. This malware is particularly sophisticated and likely to be part of an advanced, sustained attack on an organization. For example, in 2014, Dyre malware was found to be capable of capturing and transmitting data before encryption occurs. Another example is the Zeus botnet, which uses SSL communications to upgrade itself.

Another security threat is a category called Threat Indicators. These are signs that a malicious party is probing or scanning the network looking for vulnerabilities. They are evidence of potential hacks or network intrusion attempts and include anomalies in network traffic flows such as traffic travelling a path it would not normally or an unusual traffic volume. Without being able to see what is in the encrypted traffic, it is far more difficult to identify these anomalies.

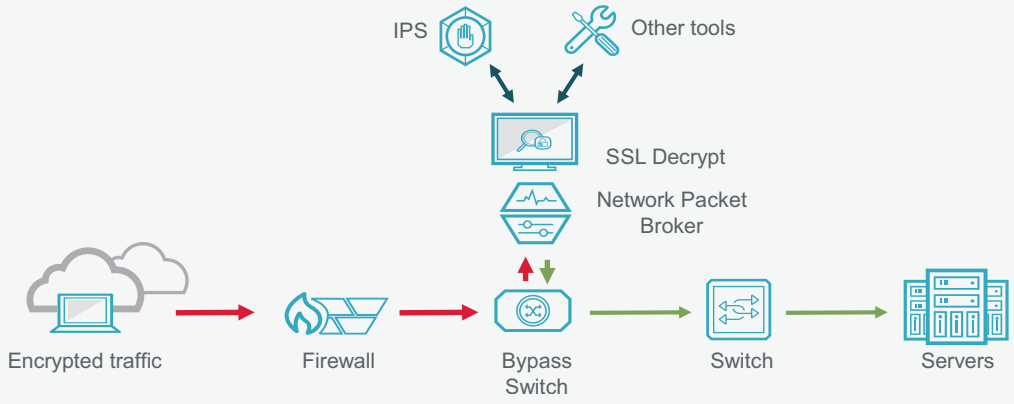
An NPB can be used to pass the encrypted traffic to an SSL decryption appliance. This solution offers complete visibility and control of encrypted traffic without requiring the re-architecture of your network infrastructure. You can add policy-based SSL inspection and management capabilities to your network security architecture to remove encrypted traffic blind spots.

8 - SIMPLIFY INLINE SSL DECRYPTION USING AN NPB WITH INTEGRATED DECRYPTION

SOLUTION SUMMARY

- Use of encryption to hide malware is growing rapidly. As of 2017, over 50% of network attacks are now hidden in SSL encrypted traffic.[13]
- SSL inspection generates a significant performance overhead on security tools
- An NPB with integrated SSL/TLS decryption capability offloads this burden without impact

Deployment scenario: Inline visibility architectures



SOLUTION OVERVIEW

Most enterprise applications are now encrypted using the SSL standard, and its updated version TLS, to thwart security attacks and hackers. Unfortunately, these bad actors have adapted to the new security defenses and are actually using encrypted data to their advantage. The bad actors are able to hide malware within encrypted data streams. Use of encryption to hide malware is growing rapidly. In fact, as of 2017, over 50% of network attacks are now hidden in SSL encrypted traffic.[13]

Integrated decryption capabilities, along with application intelligence, can be used to provide an easy and cost-effective way to examine suspect data. For instance, there is no need to have a SIEM try to correlate information from multiple sources, direct data to/from decryption tools, and then track the flow of information to security and analysis tools. Within an integrated decryption approach, the data is decrypted while it is at the NPB and then the NPB forwards the data straight to special purpose tools. Encryption details can be reported over NetFlow to the SIEM or other devices.

At the same time, the NPB has no impact on application performance. For example, this capability can be used to decrypt simple mail transfer protocol (SMTP) mail traffic and hand it off to an antiviral tool for virus/malware inspection. Other data can be decrypted and sent off to a DLP device for deep packet inspection. No resources on a firewall or other device are needed.

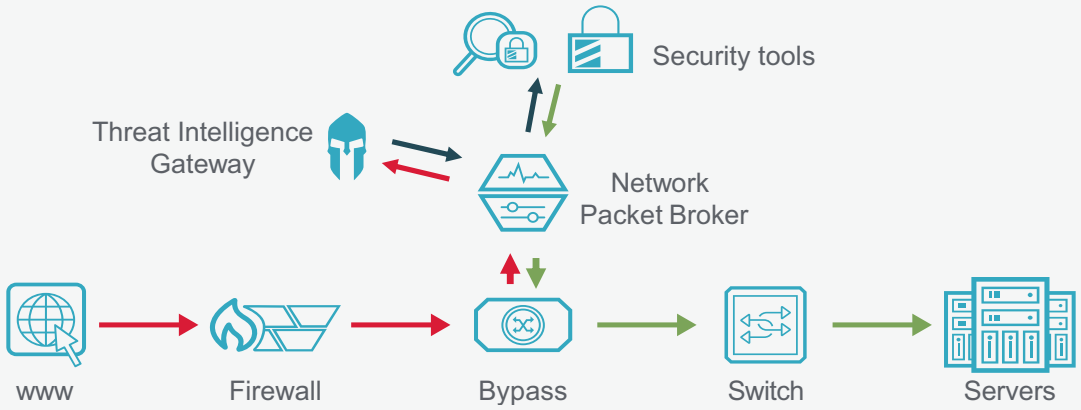
Encryption also makes troubleshooting and performance monitoring much more difficult. Integrated decryption capability allows the NPB to quickly perform this function and forward the clear data to the right troubleshooting tools for analysis. Another benefit of an integrated decryption approach is that you can very easily get a better understanding of what your network encryption strength is. Are all of your apps using strong encryption algorithms or is there a mixture of strong and weak? This lets you know how strong your security is, and is not.

9 - THREAT INTELLIGENCE GATEWAYS REDUCE FALSE POSITIVE SECURITY ALERTS

SOLUTION SUMMARY

- Security teams at large enterprises waste more than 20,000 hours per year chasing false-positive alerts[14]
- Pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30% which also reduces false positives of security breaches
- Generate return on investments (ROIs) of up to 15 times

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

Even with firewalls, IPSs, and a wide array of security tools in place, businesses still miss clues and suffer major breaches every day. Why? Because the sheer volume of alerts being generated places a huge processing drain on the security team, as well as the infrastructure itself. This translates into wasted time and money as well as an increased risk of falling victim to an attack.

A 2015 Ponemon Institute report states that security teams at large enterprises waste more than 20,000 hours per year chasing false-positive alerts.[14] By eliminating even 30% of unwanted traffic, threat intelligence could save companies some 7,000 hours per year, or the equivalent of 150 weeks in professional time. This can mean a savings of $300,000 per year, for an ROI of 15 times or higher.

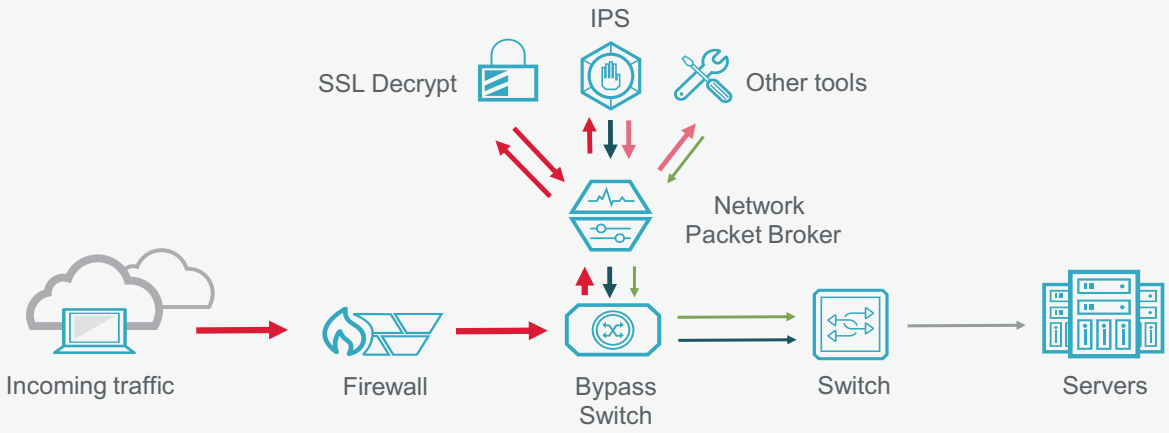
By pre-filtering known bad IP addresses and traffic from untrusted countries, you can stop unwanted traffic from ever reaching the firewall. Blocking large volumes of traffic based on IP address, location, and bad behavior enhances your security architecture performance, and reduces your team's "alert fatigue." Automatic system updates eliminate the need for manual updates of known bad IP addresses. This saves hours of configuration time over a firewall approach. Ixia's solution (ThreatARMOR) detects infected systems to thwart outbound connections with botnets, phishing scams, and malware exploits.

10 - SERIAL TOOL CHAINING OF DATA IMPROVES THE DATA INSPECTION PROCESS

SOLUTION SUMMARY

- Send data to tools sequentially for detailed analysis of suspicious data
- Serial data chaining can be powerful but is hard to implement without an NPB
- Pre-set NPB tool chains ensure that actions occur in proper sequences

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

Tool chaining is a powerful solution for automating the movement of data packets in security monitoring solutions because of the ability to partition out suspect data and pass that data through additional security inspections. The NPB is the enabler for this functionality. Suspect data can be passed back and forth between an NPB and multiple security tools (IDS, DLP, SSL, WAF, NGFW, etc.). Security tool chaining is used to deliver the interoperability needed to make network security protection mechanisms truly successful.

Security and monitoring tools are typically linked together by using software provisioning to control the flow of data through the selected services. The data inspection can be performed in parallel or in serial, depending on the situation. To accomplish the proper flow of data, one or more tools are assigned to a port or port group on the NPB. Multiple port groups can be chained together. A well-designed NPB can support complex service chaining with many tool groups in parallel, in serial, or in a combination.

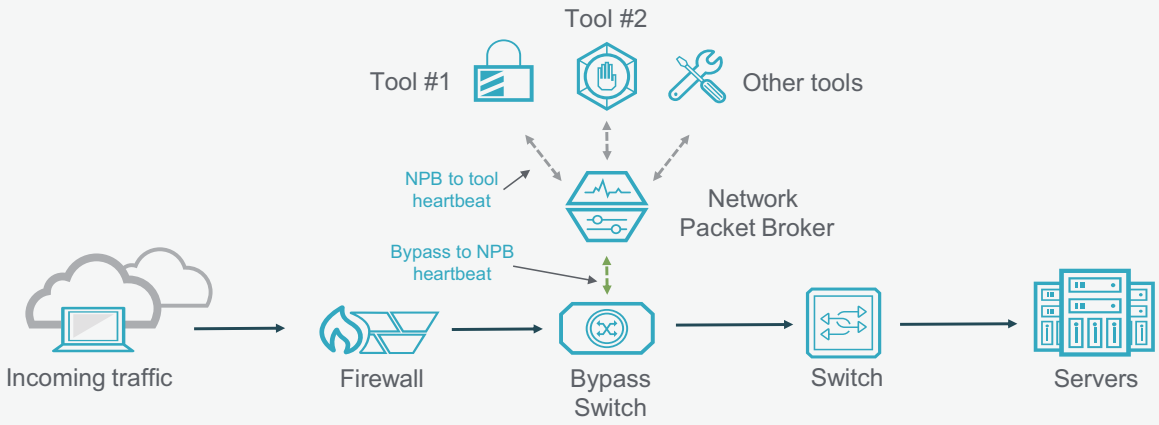
For example, data can be passed to the NPB from the bypass switch. Encrypted data can be filtered based upon Hyper Text Transfer Protocol Secure (HTTPS) and sent to a decryption device. Once the decrypted data is returned to the NPB from the SSL decryptor, it can then be passed to an IPS for inspection. Packets without anomalies are moved along quickly, to maintain maximum response time. A common example is the use of an IPS solution to filter out suspicious traffic for further analysis by other tools in the daisy-chain. Traffic without exception is quickly sent back through the network to support the fastest possible response time. Data that is flagged for more inspection can be sent from the NPB to another port group that might contain a DLP or some other device for further analysis. Based upon that analysis, the data can be killed, deemed non-threatening and passed on into the network, or it could require further analysis/quarantining.

11 - SELF-HEALING INLINE SECURITY ARCHITECTURES MAXIMIZE NETWORK AVAILABILITY

SOLUTION SUMMARY

- Business IP traffic will grow by a factor of nearly three between 2016 and 2021[15]
- Heartbeat technology in NPBs and bypass switches can help equipment create a self-healing architecture
- Negative heartbeats can validate firewalls are working correctly

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

Today's data networks are crucial to a typical business as they affect employee productivity, ecommerce, communications, etc. Because of this, data networks need more reliability. Implementing bypass switches, inline NPBs, and HA architectures is part of the solution. However, another part of the solution is to create self-healing networks.

For instance, while link-state awareness capabilities in a bypass switch or NPB provides HA for tool failures that result in down links, other types of failures may occur without downing a link. Heartbeat checking monitors the health of attached inline monitoring devices by transmitting small heartbeat packets at regular intervals out of the bypass or NPB ports that are connected to the security tool, like an IPS. The IPS is expected to pass the packet back to the transmitting device. If the bypass or NPB does not receive the returning heartbeat packets within a heartbeat interval, and after a specified number of retries, the IPS is considered down. Typical heartbeat intervals are 100 ms with a minimum of two retries but this is customizable. The NPB will continue to issue heartbeat packets to the IPS, and as soon as returning Heartbeat packets are received, the IPS is considered up and traffic will resume flowing in that direction, creating a self-healing loop. If the heartbeat message is not received and only a bypass is installed, and no redundant IPS, then the bypass can initiate a fail-over to allow the network to remain up. Once heartbeat messaging returns, the bypass functionality is disengaged.

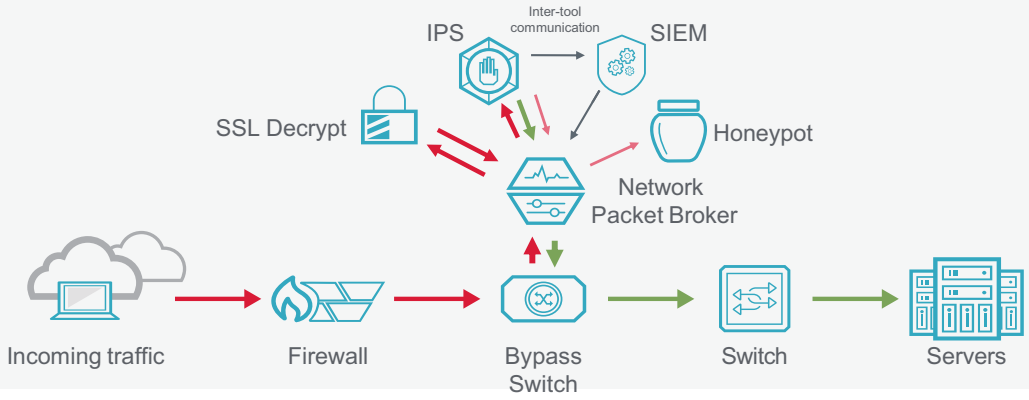
Multiple layers of heartbeat messaging can be created. For instance, one layer between the bypass switch and the NPBs and a second layer between the NPBs and the tools. In addition, different heartbeat signals can be used. The case just described is the normal heartbeat. A second type is called a negative heartbeat. In this situation, the NPB sends a "threat" heartbeat to a firewall. Normally, the firewall should block the heartbeat since it is a threat. However, if the firewall starts to pass the heartbeat, then there is either a configuration error on the firewall, or it is in failure mode that allows packets to pass freely through it. If the NPB detects that the negative heartbeats are appearing, then it will stop sending traffic to that firewall. If the heartbeat cannot penetrate the firewall, this means the tool is alive and working as expected.

12 - PROTECT YOUR NETWORK WITH AN NPB AND A HONEYPOT

SOLUTION SUMMARY

- Since security threats continue to morph, the deception technology market continues to grow at a compound annual growth rate of 9%[16]
- Decrease IPS false negatives and positives by deploying a honeypot
- An NPB can be used to divert suspect traffic to a honeypot for further analysis

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

A honeypot is a purpose-built area designed to lure in network hackers to study how they gained entry into a network, what they are looking for, and observe the various threat vectors they are employing. This device is walled off from the main corporate network, but it should mimic the production environment to give a realistic experience. While professional security organizations and agencies may actively try to lure hackers to their honeypots, most enterprise and service providers hope that this is something that never gets used. However, in the event of a network breach, you want to be able to steer a hacker away from the real network and over to this decoy area for containment and observation.

A properly designed visibility architecture with inline bypass switches and NPBs can be used to capture network data associated with a breach and direct that data to specific security tools, like an IPS or DLP, for analysis. Once suspicious data is identified, it can either be killed or directed to the honeypot for analysis. The use of honey pots can also take the burden off of your IPS and decrease the number of false positives and negatives for security threats.

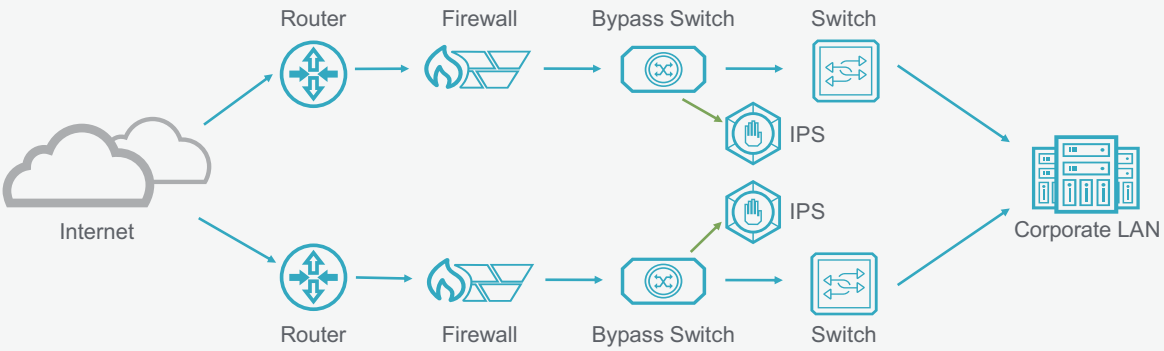
The criteria for flagging the bad data is determined by the IPS, which is connected to a SIEM. Based on exchange of that information, the SIEM typically makes the decision that the data from a particular IP address is bad and communicates it to the IPS, which can then tell the NPB that data with a specific source and destination IP addresses is bad. The NPB can then send that specific data out a tool port, which is connected to the honeypot. Alternatively, the SIEM could communicate directly to the NPB through a Representational State Transfer (REST) interface to divert that packet data to the Honeypot.

13 - SAVE TIME AND MONEY WHEN DEPLOYING ASA FIREWALL MIGRATIONS

SOLUTION SUMMARY

- 5 to 10% of all network downtime is associated with network maintenance[17]
- Use a bypass switch for fail-safe migrations to Cisco FirePOWER security appliances
- Cut deployment times for FirePOWER upgrades from 4 hours per tool to 4 minutes[18]

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

Network architectures continually change. One of the newest improvements is to add an NGFW to increase application security. Other solutions, such as an IPS have been around longer. In fact, the list of inline security tools is growing rapidly. ZK Research estimates that enterprises deploy an average of 32 different security solutions in their network.[19] If the inline tools are deployed directly into the network, the maintenance of this solution becomes a nightmare. The simplest, and most effective, remedy is to insert bypass switches before the devices that provide an easy fail-over mechanism for maintenance-related activities.

Maintenance windows are precious. The amount of time for the window is usually only a few hours, and the downtime has to be scheduled and approved by a Change Control Board. Time between windows can take weeks so the window must be maximized. When it comes time to upgrade your Cisco Adaptive Security Appliance (ASA) to a dedicated FirePOWER appliance, you want to minimize the time spent configuring a resilient path for FirePOWER upgrades. A typical IPS install can take anywhere from 2 to 4 hours, which is a lot of downtime.

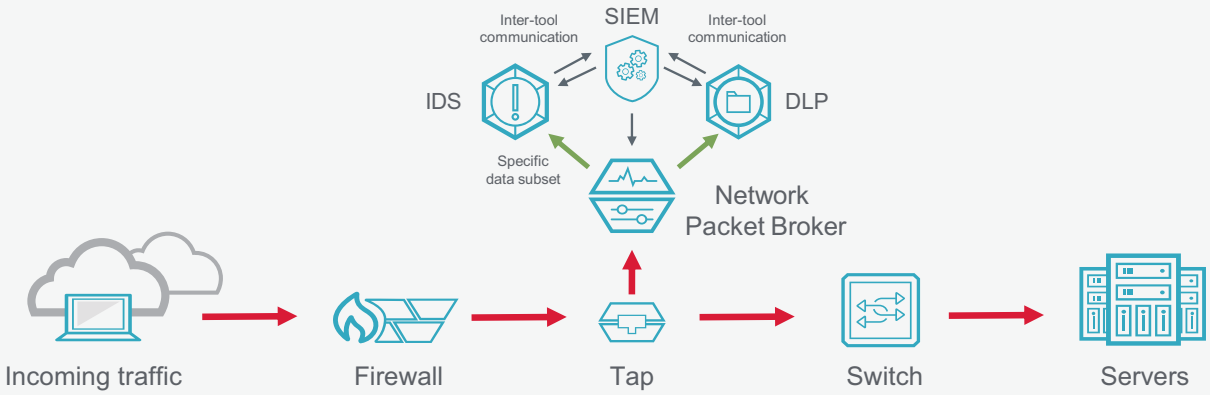
The solution is to install an Ixia external bypass switch, which takes only about 4 minutes, since it is already preconfigured for Cisco solutions. This allows you to cut the deployment time for a FirePOWER upgrade from 4 hours per tool to 4 minutes. Using the bypass switch in tap mode, traffic can still flow in your live network while also being replicated to the FirePOWER IPS. Once the IPS is configured, tested, and ready for deployment, it can be easily placed inline with no further network disruption. The benefit to network downtime from using an external bypass becomes significant when you have dozens of IPS upgrades.

14 - SIEM INTEGRATIONS AUTOMATE THREAT DETECTION AND MITIGATION

SOLUTION SUMMARY

- SIEMs use log data to detect anomalies
- NPBs can automatically respond to SIEM REST calls with actions in near real-time
- Faster responses to problems result in faster incident detection, faster MTTR, and reduced risk

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW:

Dynamically changing security threats mean that what an enterprise needs to monitor is constantly changing. In addition, increasing network speeds makes it impractical to perform deep packet inspection on all traffic. Automation of network monitoring allows you to align your tools with dynamic network changes to increase operational efficiencies and create an adaptive monitoring environment.

SIEM solutions are powerful tools that can be used to assist in this area. SIEMs use log data to provide a wide view of the network and have powerful correlation capabilities to detect anomalies. However, SIEMs do not provide packet-level visibility to analyze anomalies in detail. While most enterprises currently use their SIEMs for reporting and compliance, mitigation is an up-and-coming use case. Packet-based tools like forensic recorders, IDS and Sandbox solutions provide needed detail, but it is not often practical to deploy them everywhere.

A SIEM integration allows customers to leverage their investments in SIEM and packet-based tools to dynamically adjust what they monitor and protect. Some of the SIEM solutions on the market include: IBM QRadar, MicroFocus ArcSight, LogRhythm, and McAfee. Manual processes are automated to speed incident detection and mitigation. Operational expenditures (OPEX) and capital expenditures (CAPEX) costs are also reduced.

This adaptive monitoring solution allows the automated data center controller to send commands to an NPB using a RESTful interface to initiate various functions (e.g., apply filters, add connections to more tools, etc.) in response to external commands. REST application programmable interface (API) calls from the SIEM reconfigure the NPB to send traffic of interest to any connected security tool.

Cost Containment

NETWORK VISIBILITY CAN PROVIDE COST REDUCTION CAPABILITIES WHILE INCREASING EFFICIENCY

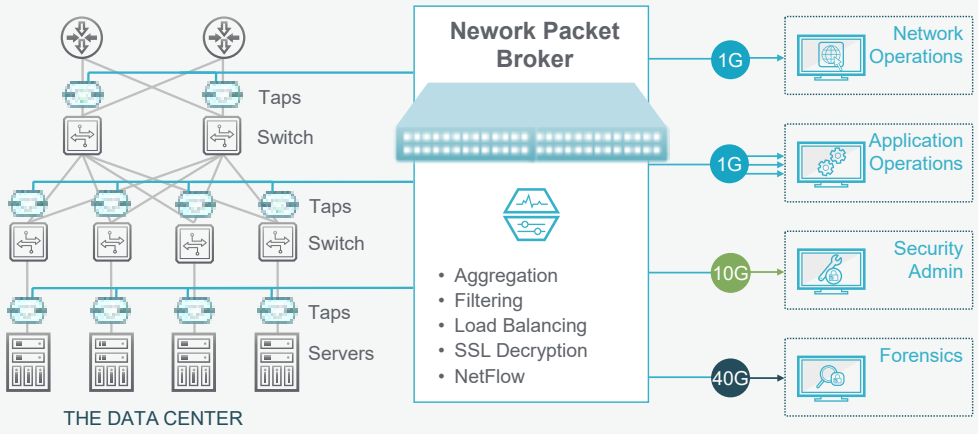
ixia
A Keysight Business

15 - NPB-BASED DATA FILTERING ALLOWS MONITORING TOOLS TO SCALE EFFICIENTLY

SOLUTION SUMMARY

- Filtering of monitoring data is one of the most commonly used NPB features
- It can significantly reduce the amount of unnecessary data sent to security and monitoring tools which increases tool efficiency and allows them to scale

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

This solution illustrates how the data captured as part of your visibility architecture needs to be optimized, i.e., edited before transmission to monitoring tools. To accomplish this, the monitoring data is sent to a central collection point, called a network packet broker. Since the data coming in from the tap is a complete copy of all data, some of it will need to be filtered before being sent on to the appropriate monitoring tool. Filtering means only the "right" information is sent to the tools, and it can be segmented out so that only certain pieces of information go to specific tools. Depending upon your monitoring needs, 90% or more of the data can be quickly and efficiently removed to maximize monitoring tool efficiency and scale.

When considering a network packet broker, it is important to understand its filtering capabilities. Filtering is usually performed in three stages. The first stage is performed at the port where the network is attached (network port). The second stage is a highly capable, port-independent filter that is located between the network port and the port to which the monitoring tool is attached (tool port). The third stage of filtering is performed at the tool port itself. Three-stage filtering is important because filtering at the network port completely eliminates the excluded traffic from being available to all tool ports. Once this traffic is removed, it is no longer available for analysis.

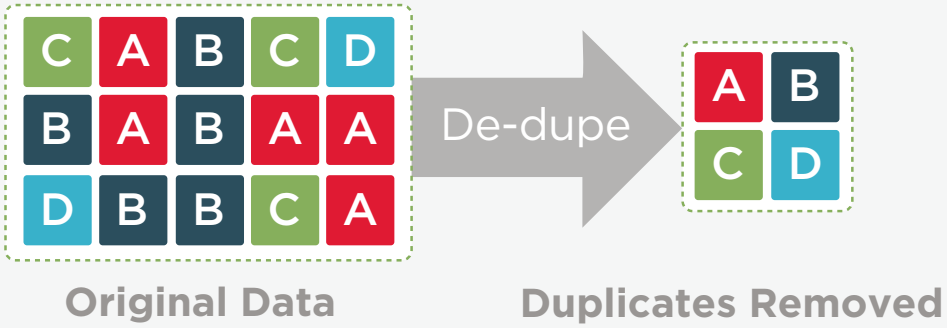
An alternative to this approach is to only filter data at the tool port, but this causes two problems. First, the tool port can be overrun by the volume of traffic coming from the network ports. Second, the interaction between the network filters and the tool filter is complex and not obvious unless you are well versed in set theory. The port-independent filter is the ideal place to perform the bulk of the filtering, as it is possible to understand exactly what is happening by looking at this single filter definition.

16 - DEDUPLICATION INCREASES MONITORING TOOL EFFICIENCY AND ACCURACY

SOLUTION SUMMARY

- Even when optimally configured, a SPAN port may generate between one and four copies of a packet
- Cisco ACI architectures create a significant amount of duplicate packets
- NPB deduplication reduces the amount of filtered data sent to tools
- Tool efficiency increases of 30 to 50% improvement have been seen[20]

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Duplicate packets of monitoring data can come from several sources, including the use of SPAN ports and the geographic location of data captures. For instance, a normally configured SPAN port (which is frequently used to connect monitoring tools to the network) can generate multiple copies of the same packet. These copies are exact duplicates of the original packet. Even when optimally configured, a SPAN port may generate between one and four copies of a packet, and the duplicate packets can represent as much as 50% of the network traffic being sent to a monitoring tool. Eliminating this unnecessary data improves the capacity of pertinent data that your monitoring tools can process.

It also matters where you capture monitoring data. If you capture it at the ingress and then again in the core, you may have copied the same data twice. This double capture is in addition to whatever duplicates were made by the core switches themselves. Cisco ACI architectures have multiple tap points that generate a significant amount of duplicate data which needs to removed. If not removed, monitoring tool costs become exorbitant to process the excess data.

Advanced context-aware data processing features, like deduplication, within a packet broker can remove these duplicate packets. The NPB is capable of removing duplicate packets at full line rate before forwarding traffic to the monitoring tools. Multiple copies are simply dropped from the data stream with no effect on the tools. A large deduplication window and the ability to configure the window size within the NPB makes the deduplication feature extremely powerful.

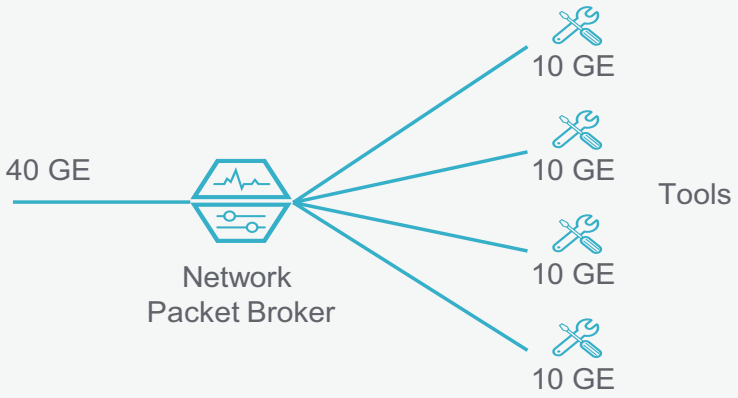
Some tools can do this, as well. The issue with the tool doing performing deduplication is that you are now spending tool CPU resources and time to perform this function. This slows down the processing capability and might even necessitate buying another tool to handle the extra load. Since tools are often expensive, this can become a costly choice. A packet broker is usually a more cost-effective alternative.

17 - LOAD BALANCING EXTENDS THE LIFE OF 1/10GBPS TOOLS IN 40GBPS NETWORKS

SOLUTION SUMMARY

- Data from EMA shows that 32% of enterprise tools are underutilized[21]
- Use an NPB to pool your tools and then load balance across them—fewer tools required and less cost
- Media speed conversion (40 Gbps to 10 Gbps) spreads 40 Gbps loads across multiple lower rate tools to extend the life of those existing lower rate tools

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Another very important use case for decreasing costs is load balancing. There are a couple clear examples of how load balancing can help most enterprises. First, network traffic increases, along with traffic speed increases, are a very common occurrence. But what about the monitoring impacts of the bandwidth upgrades? For instance, if you upgrade your network core from 1 Gbps to 10 Gbps, you will now need 10 Gbps tools to properly monitor it. If you upgrade to 40 Gbps or 100 Gbps, there may be few to no monitoring tools available at those data rates. And available tools at those data rates can be very expensive.

Packet brokers provide the aggregation and load balancing capabilities needed. Data coming into the packet broker can be broken down into lower rate streams of data and then sent to the proper monitoring tools. For instance, load balancing of 40 Gbps data allows you to spread the monitoring traffic across multiple 10 Gbps tools if you need to. This obviously assumes you have enough 10 Gbps tools for the load. Once you implement this, you can extend the life of your 10 Gbps tools a little longer until you have enough budget to purchase more expensive tools that can handle the higher data rates. For instance, you might implement the network upgrade you want to this year and then purchase additional higher-rate monitoring tools later.

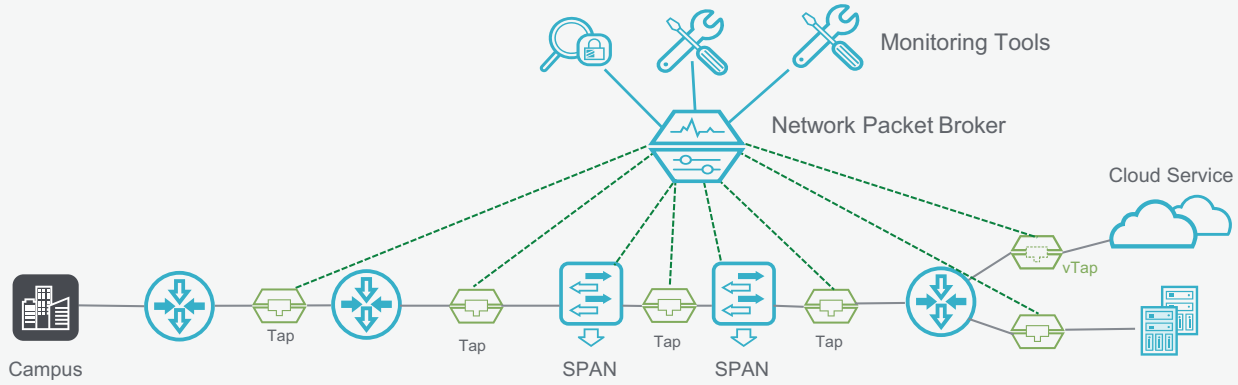
Another example is to pool your tools in one location and feed them the data they need from a packet broker. Some architectures use individual tools spread out across the network. This may have some minor access advantages, but these tools are often underutilized. 2016 survey data from Enterprise Management Associates (EMA) shows that 32% of enterprise tools are under-loaded, i.e. less than 50% utilization.[21] Tool centralization and load balancing allows you to pool your tools and increase this utilization by using fewer tools. You can often postpone purchases of additional tools until the utilization factor is high enough to warrant additional tools.

18 - MAXIMIZE MONITORING TOOL EFFICIENCIES WITH DATA AGGREGATION

SOLUTION SUMMARY

- Data from EMA shows that 32% of enterprise tools are underutilized[22]
- Create access to multiple areas of the network for your monitoring tools
- Use an NPB to aggregate monitored traffic from multiple links to maximize monitoring tool utilization

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Network blind spots are an extremely common problem for all businesses. These blind spots are areas where you do not actually see everything that is happening on your network. They are often caused by a lack of visibility. A common fix for the blind spot problem is to simply add more security and monitoring tools. However, just adding more tools leads to even more problems. One example is that you need to monitor multiple segments of your network to truly understand what is happening. When you add more tools, you also have to distribute them across the network so that they have access to monitoring data. Unfortunately, this ends up where the tools are typically underutilized. It is not uncommon to end up with only about 10 to 30% utilization of the CPU for each tool. This results in low tool utilization (i.e., undersubscription) and a corresponding low ROI for your tool investment. So, for most of the time, the tool sits idle. That is like buying a fleet of 12 cars to use for a whole year but you only use each car for a total of 1 month during the year—you did not get any value for the other 11 months, just expense.

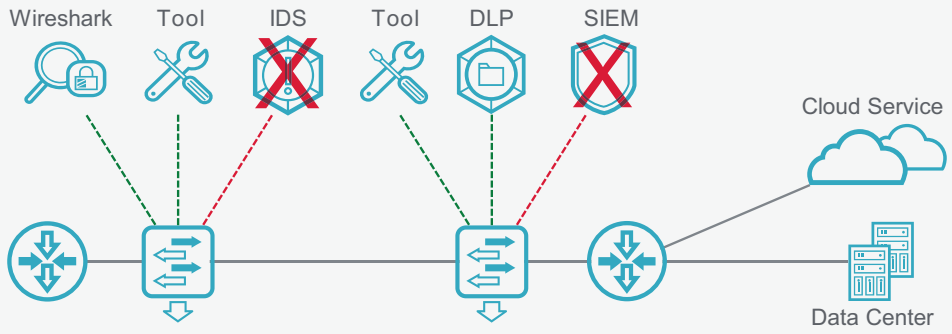
While adding tools and data access points is definitely part of the solution to blind spots, you also need to add an NPB to filter and groom the data before it is sent to the monitoring tools. NPBs allow the aggregation of multiple ingress links to one egress port for a specific tool. This allows you to pool your tool resources for multiple individuals and departments to use. Now, you have cost effective data access and filtering across the network.

19 - ELIMINATE SPAN PORT CONTENTION ISSUES

SOLUTION SUMMARY

- Most routing switches come with two SPAN (mirroring) ports which is typically not enough to feed data to all of your monitoring tools
- An NPB eliminates the issue and reduces monitoring strategy costs by sharing traffic data with all desired analysis and monitoring tools
- An NPB makes it easier to add/remove new monitoring tools

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Most routing switches contain two switched port analyzer (SPAN) ports. These ports can be programmed to mirror a copy of routed traffic from one of the routing switch ports. Depending upon programming, data from switching ports can be mirrored to the SPAN port. However, bandwidth limitations apply. Once the traffic is mirrored to a SPAN port, a security or monitoring tool can be connected to that port to process data.

However, when the number or capacity of SPAN ports is reached, no more tools can be connected. Since the number of configured SPAN ports is normally two, this means that only two tools can be connected to the switch. Since most enterprises use far more than two tools, (survey data from EMA shows that the typical enterprise uses up to 15), visibility blind spots in the infrastructure are usually created.[22] There is often contention within the enterprise for access to the SPAN ports. Adding or reconfiguring SPAN ports results in additional cost and delay in providing full visibility to all your security systems.

Connecting an NPB is a quick, simple, and cost effective way to resolve the problem as it allows traffic to be distributed and inspected by many monitoring tools at once, since the NPB has plenty of ports for distribution of data to multiple tools simultaneously.

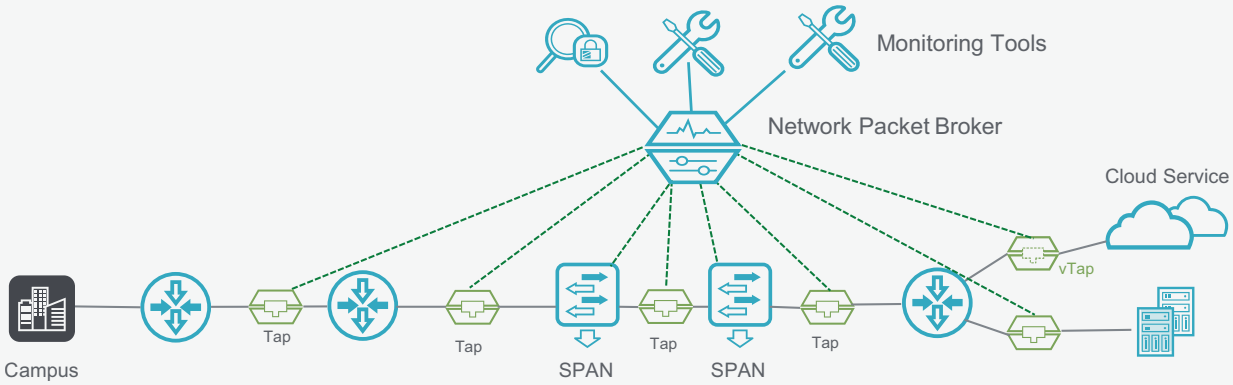
An Ixia case study shows the various problems that a national pharmacy ran into with SPAN port contention problems.[23] The case study also shows that the customer ran into problems splitting and filtering the data natively from the SPAN ports. A visibility architecture solved the problem.

20 - INCREASE TOOL EFFICIENCY BY COMBINING VIRTUAL AND PHYSICAL MONITORING

SOLUTION SUMMARY

- Over 70% of enterprise workloads are virtualized[24]
- Virtual data and physical data can be combined and exported to the same NPB for distribution of data to existing security and monitoring
- CAPEX spending can be controlled by maximizing the capabilities of your existing tools

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

A common occurrence now is the use of virtual machines. Virtualized servers and cloud networks are ushering in a new era of cost savings but also complexity. Virtual data can be hard to access and can become expensive to analyze. Most companies already have a set of security and monitoring tools for the traditional, i.e., physical, network. Adding virtual tools (e.g., virtual firewalls, security inspection, and performance monitoring) can become an expensive duplication in cost and monitoring efforts. This can also create a siloed approach to network monitoring, since managerial ownership of the virtual data is typically separate from the network monitoring group.

A cost-effective solution is to add a virtual data access device, i.e., a virtual tap. A virtual tap is a software version of the hardware tap that can be used for VMware, KVM, Hyper-V, and cloud. environments. The virtual tap is loaded into a virtual machine (VM) on the server. Once there, it allows you to export monitoring data outside of the virtual environment to an NPB using Generic Routing Encapsulation (GRE) or a VLAN tunnel where the data can be filtered by the NPB, aggregated with other monitoring data, and then distributed to the appropriate security and monitoring tools in the physical data center.

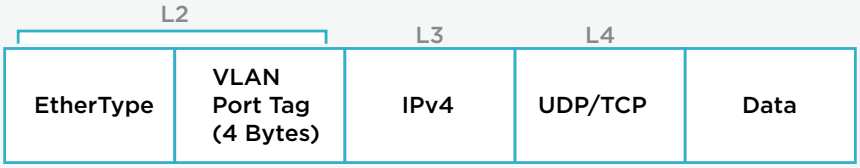
Once data from the physical and virtual data centers are combined, companies can achieve economies of scale by maximizing the utilization of the tools you have current investments in. In addition, the combining of the data gives you a better understanding of the network. Instead of looking at the performance of the different pieces of your network, you can get a combined view from the consolidated data. The consolidated data also gives you better control of your regulatory commitments, because you will have better confidence that you have applied consistent regulatory practices across the whole data center, not just piece parts. Non-compliance in one area is still non-compliance for the company.

21 - TRACK YOUR MONITORING DATA TO OPTIMIZE NETWORK PERFORMANCE

SOLUTION SUMMARY

- An NPB is a key component for optimizing network monitoring data
- Port tags associate data to a specific NPB port to document data origin for improved forensic analysis
- Port tags can identify specific customer data in multi-tenant environments
- Timestamps can help detect network and monitoring tool analysis delays

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Capturing relevant data is a key component of a network monitoring strategy. At the same time, being able to track specific kinds of data and determine the origin of that data is equally important. This provides context and more relevance to the monitoring data. This is where an NPB can provide value-add capabilities, such as network port tagging, VLAN tagging, and timestamping to help identify and characterize monitoring data.

There are several common use cases for port tagging and timestamping. These include improved forensic analysis, multi-tenant data tracking, and data-event correlation. The port tagging feature, in conjunction with the existing precision timestamping feature, allows customers to perform forensic analysis of network data captured from a large number of monitored segments without losing visibility into the origin of the traffic.

Port tagging is used to identify input data streams and associate that data to a network port on the NPB. If the input data is segmented to specific ports, this allows you to know what data type came from where. In a situation where multiple network ports are aggregated to a single tool port at egress, you can use port tagging to identify which network port each packet arrived on during ingress. This can be performed on a single NPB or in multiple NPB environments. The picture above shows where a VLAN port tag is added to the packet (as an outside header to the Layer 2 information after the EtherType and is four bytes long) for tracking purposes. The VLAN identification (ID) of that header typically represents the network port number, but you can also create a custom VLAN ID.

Custom port-tagged VLAN IDs can also help you minimize potential conflicts if you also use the deduplication packet processing feature. When using both port tagging and deduplication, if packets arrive from two network ports where the only difference is a VLAN header, where one packet has a VLAN header while the other does not, and the port tagging feature adds a VLAN header that is the same VLAN ID as the other packet, then the packets could become duplicates, and one of them could be stripped if they both egress a tool port where deduplication is enabled.

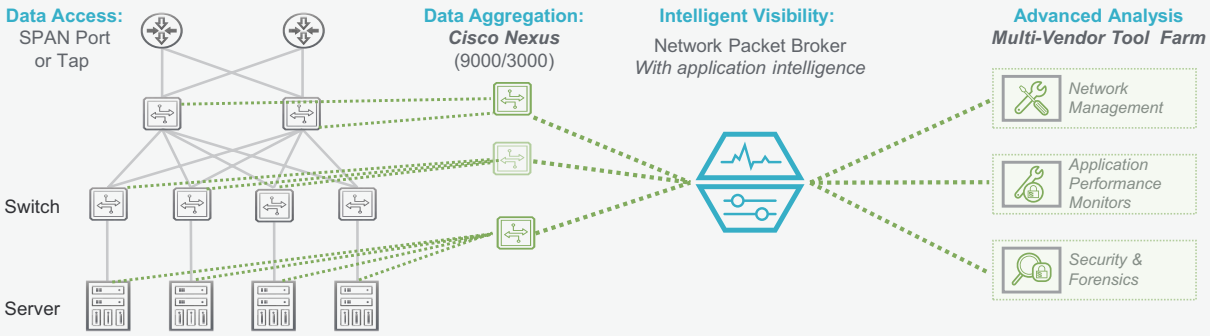
Network operators also require high-accuracy timestamps on packets to correlate events with other device logs in low-latency financial data centers and to correlate traffic events across a wide-area network (WAN). Timestamp sources include: local, network time protocol (NTP), and precision time protocol (PTP). The NPB can then insert a high-accuracy timestamp into every packet at ingress.

22 - OPTIMIZE NETWORK TRAFFIC WITH CISCO NEXUS 3000/9000 INTEGRATION

SOLUTION SUMMARY

- Optimize the network traffic distributions to make better use of IT tools
- Cisco Nexus switches can be used as a distributed data aggregation layer
- Network administrators will have a single pane of glass management system that allows them to program selected Cisco Nexus ports from an Ixia NPB for improved monitoring data captures

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

The Cisco Nexus 3000 network switch family offers low-latency, high programmability, and high-density switches in a fixed compact form factor. The Cisco Nexus switches also use a common programmatic interface. Ixia NPBs can integrate directly with a Nexus 3100 switch through the logical aggregation group (LAG) port. This provides a management interface to those Cisco switches through the Ixia user interface. It also allows network administrators to dynamically repartition Cisco switch ports between production switching and visibility enablement without having to leave the Ixia monitoring solution. As a result, customers can optimize infrastructure utilization and reduce overall visibility costs.

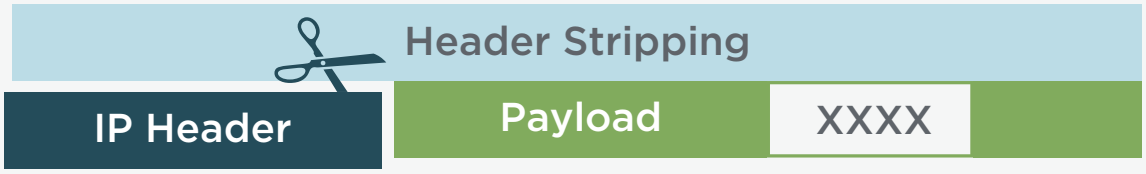
The Cisco Nexus 3000 switches can be used as a data aggregation layer to provide access to network monitoring data from distributed locations throughout your network. The NPB integrates data from the different locations, filters that data, and then distributes the resulting data to the appropriate monitoring tool. The NPB aggregation function consolidates the monitoring data, which results in optimizing the efficiency of existing monitoring tools and subsequently decreasing the need for additional monitoring tools. At the same time, the Ixia management system allows for dynamic data monitoring and troubleshooting on segments with the Cisco switches. The alternative would be to physically connect tools to the individual Cisco switches (during maintenance windows) to perform troubleshooting. Ixia is the only visibility vendor to provide an integrated solution using our own equipment combined with Cisco Nexus 3000/9000 switches.

23 - HEADER STRIPPING INCREASES EFFICIENCY OF MONITORING TOOLS

SOLUTION SUMMARY

- At least 7% of monitoring implementations require header stripping[25]
- ACI adoption and use of VXLAN will continue to drive this use case
- An NPB can be used to easily remove unnecessary IP packet headers

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Header stripping, also called de-encapsulation, is the removal of various types of extraneous routing information or other information contained in the packet header that has no monitoring value. Examples include: MPLS labels, VLAN tags, Virtual Extensible Local-Area Network (VXLAN) protocol, and GTP information. While the information is useful from other aspects, from a monitoring tool perspective, it is uninteresting and confusing. If monitoring tools do not understand the header information, those packets end up getting thrown away.

Network packet brokers can be used to remove this header information before the monitoring data is sent to the monitoring tool. This makes the monitoring tool more efficient, and in some cases, actually allows the monitoring tool to function correctly.

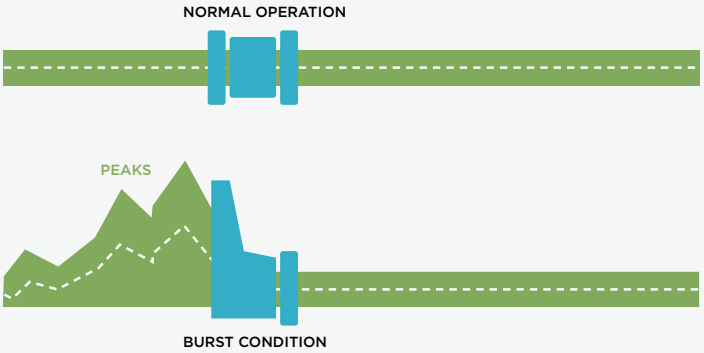
For instance, most monitoring tools are not capable of understanding MPLS-tagged packets, making them unable to monitor MPLS networks. An NPB can remove the MPLS headers and forward the original packet contained within the MPLS tagged packet. Standard network monitoring tools can then be used to monitor activities within the MPLS network. Removing MPLS labels is a form of off-loading that increases the capability of monitoring tools.

24 - PROTECT MONITORING DATA WITH EXTENDED BURST PROTECTION

SOLUTION SUMMARY

- Ethernet has inherently bursty traffic patterns
- You need to see every packet, even under microburst conditions
- An NPB with extended burst protection uses buffering to overcome packet delays

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Ethernet is inherently bursty. When real-time protocols like VoIP are added to the mix, traffic burstiness can become noticeable and result in network equipment buffer overloads and IP packet loss. There does not have to be catastrophic failure for packet data to get lost. For instance, there could be network congestion due to a high-volume of traffic. There could also be delays caused by the use of slower speed equipment, i.e., 1 GE equipment in use on 10 GE networks. Another source of packet loss could come from overburdened inline security tools or overburdened routing switches. Whatever the cause, packets can become delayed or lost on the network.

One solution to this situation, if it occurs on the monitoring network, is to be able to deploy deep buffering (also called extended burst protection) of up to 200 MB on an NPB. This deep buffering allows monitoring tools to see every packet, even under microburst conditions, where aggregate bandwidth temporarily exceeds port capacity. The condition commonly occurs when traffic from a high-speed network is adapted to feed a lower-speed tool.

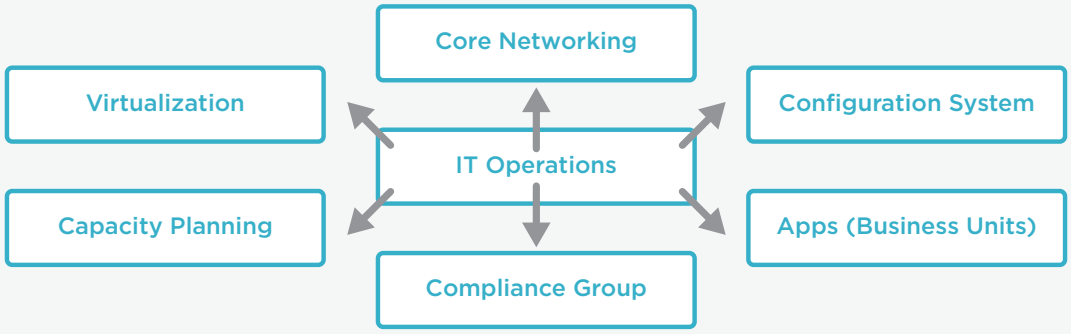
Extended burst protection in the NPB offers traffic management and protection to online businesses that are subject to bursts of activity. For instance, stock trading, online betting, and gaming are examples of industries where companies may want to deploy extended burst protection to limit packet loss. This speeds up data analysis by monitoring tools and can potentially decrease traffic on the network (due to retransmissions).

25 - NPB AUTOMATION DRAMATICALLY IMPROVES MONITORING RESPONSE TIMES

SOLUTION SUMMARY

- NPBs can automatically respond to network incidents with actions in near real-time
- Faster responses to problems result in a shorter mean time to diagnosis and a corresponding faster MTTR
- REST is used to issue commands from an NMS, SIEM, policy controller, or orchestration system for security incidents, network incidents, or equipment changes

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

The days of static programming are coming to an end. Automation of network monitoring allows you to align your tools with dynamic network changes to increase operational efficiencies and create an adaptive monitoring environment. This automation capability creates a tight integration between automated data center provisioning systems (network management system (NMS), operational system support (OSS), or other orchestration system) and your existing tools (e.g., network monitoring, application monitoring, security analysis, etc.).

Specifically, the solution allows the automated data center controller to send commands to an NPB to initiate various functions (e.g., apply filters, add connections to more tools, etc.) in response to external commands. This automation is akin to software-defined networking (SDN). However, the source of the command does not have to be an SDN controller. It could be a NMS, provisioning system, SIEM tool or other management tool on your network. Automation events can be triggered in response to internal events (based upon some filter parameter or event monitoring parameter) or external events (such as Simple Network Management Protocol (SNMP) traps, SNMP polls, Syslog, NMS events, SIEM events, or other software tool that supports a RESTful interface or Tcl scripting).

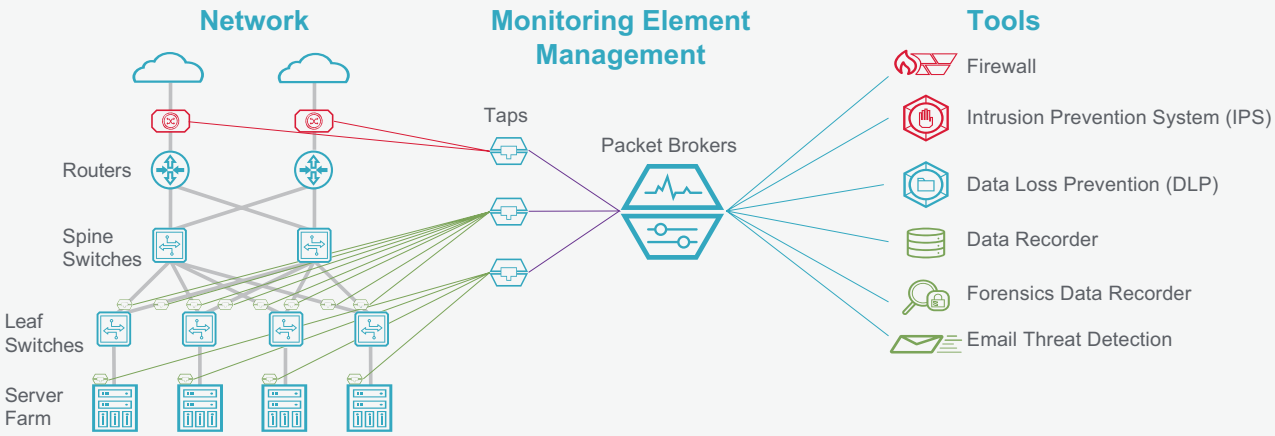
There are typically two main groups within IT that need adaptive monitoring—the IT operations group and the tools group. The main driver for the operations group is achieving operational efficiency to reduce manual processes and the delays/errors that those processes introduce. For the tools group, the main driver is increasing the monitoring capability for the whole network because most IT departments usually do not have enough money to provision multiple sets of tools across the whole network.

26 - REDUCE TCO WITH EFFECTIVE VISIBILITY ARCHITECTURE MANAGEMENT

SOLUTION SUMMARY

- Proper remote management of devices can reduce troubleshooting time up to 75%[26]
- The OPEX for monitoring equipment can make or break a solution TCO
- A visual drag-and-drop interface simplifies filter creation by reducing the time needed
- A single pane of glass makes managing multiple NPBs easier

Deployment scenario: Inline and out-of-band visibility architecture



SOLUTION OVERVIEW

One of the most critical components of a visibility architecture is the long-term management of the solution. The element management system (EMS) component contributes heavily to the total cost ownership (TCO) of a visibility solution. In fact, proper remote management of devices can reduce troubleshooting time by up to 75%.[26] The EMS is used to configure individual network elements (NPBs, virtual taps, etc.) that are part of the visibility architecture. It is also used to set up the inline and out-of-band architecture components and programming.

One of the most important benefits of the EMS is that it gives you a single pane of glass from which you can perform filter, policy, user, and device management. The interface can be used for configuring one element or multiple elements (NPBs, bypass switches, application intelligence, SSL decryption, etc.).

Device access and filter creation can be performed directly or remotely. This saves a significant amount of time in that the engineer/IT Admin does not need to drive in to the office or remote location to make software changes. In addition, the EMS should allow you to set up groups and attach permissions to groups and filters. This allows you to create role-based permissions for filters so that others can not alter those filters without permission. This in turn eliminates unexpected surprises during troubleshooting and other activities. In a separate instance, filters can be created and placed in a library so that everyone can access them and use the same filters to guarantee accuracy and create repeatable results.

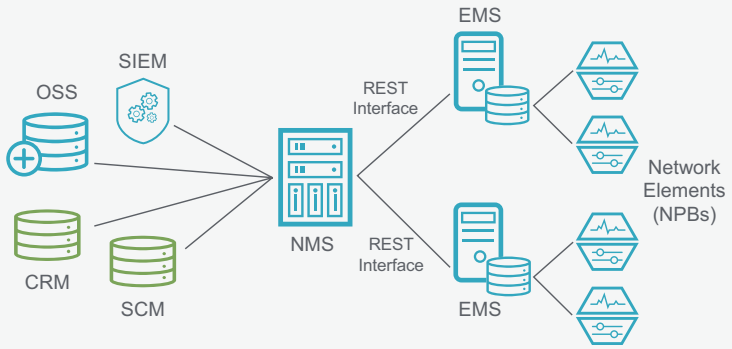
The EMS capability solves some of the biggest problems facing network administrators—remote access, a single interface to see and program multiple devices and filters, role-based permissions for improved security and compliance policy adherence, and creation of monitoring data statistics and event information.

27 - LOWER YOUR OPEX BY INTEGRATING MONITORING AND NETWORK MANAGEMENT

SOLUTION SUMMARY

- Monitoring equipment OPEX can make or break a solution TCO
- Scale monitoring equipment as needed with a single user interface
- Upgrade configurations from a central location with logging and change control
- Support orchestration initiatives within the business to reduce costs

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Enterprises need scalable and flexible networks that can adapt to the changing needs of the business world. Not only does the IT department need to add the right types of monitoring equipment (like monitoring tools, diagnostic tools, tools specific to company initiatives such as Bring Your Own Device (BYOD) and private cloud, etc.), but they need to control costs by managing their visibility architecture. In a distributed environment, such as a multi-building campus, Top-of-Rack (TOR), or End-of-Row (EOR) data center scenario, this becomes rapidly untenable. The solution is to add multiple distributed components that have the look and feel of one system and can be spun up with other network management functions, like scheduled task management, updates and backups, add/delete of users, and REST-based northbound and southbound interfaces for connection to a NMS, orchestration system, or OSS.

A centralized management approach gives you several core benefits:

- Interconnection with North bound interfaces to manage visibility components and interface to an NMS, orchestration system or OSS
- Capture of performance and statistics
- Push down of policy-based device information and filter information
- Role-based access for enhanced security
- Monitoring for device health and status
- Backup, restore, upgrades, and other services
- High availability support

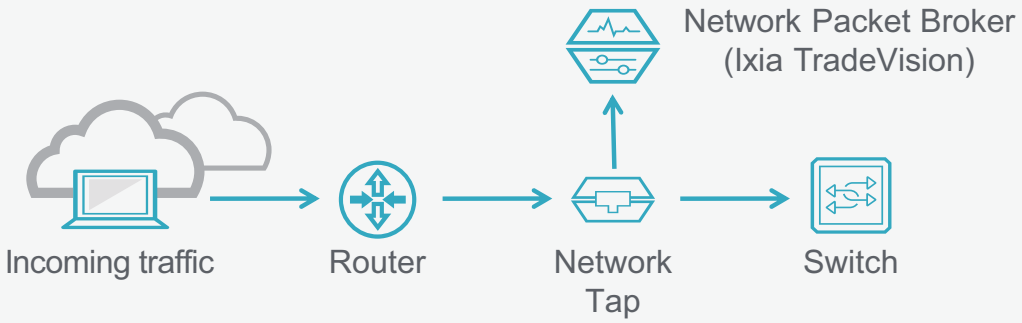
This solution allows an NMS (versus and EMS) to control multiple Ixia solutions (NPBs, bypass switches, etc.). A REST-based interface is used allow network management solutions like an NMS or an orchestration system to send commands directly to visibility architecture devices. This type of architecture solves some of the biggest problems facing network administrators—rapidly increasing scale, flexible deployments, and the need for application and security monitoring spanning the entire network.

28 - VALIDATE LATENCY FOR HIGH-PERFORMANCE FINANCIAL MONITORING LINKS

SOLUTION SUMMARY

- Milliseconds of time are worth millions of dollars to stock traders[27]
- Conduct high-performance monitoring of financial market data feeds with an NPB
- Instantly detect multicast sequence gaps and microbursts

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

The rapid detection of degradation in the quality of financial data feeds is a considerable challenge for any market participants who use or transport real-time market data. Market data transport technology is primarily based around the use of multicasting, which does not have any error correcting mechanisms at the network layer. This means that any packets containing key trade data that have been lost cannot be detected until they are passed through a feed handler system at the end user site.

This configuration has a number of issues:

- Application teams may be aware of the problem, but the tools they use may not be available to the network operations teams who are responsible for diagnosing and resolving the issue.
- Many feed handlers use feed arbitration (between A and B feeds) to autocorrect message drops, so application teams may neither be aware of problems nor able to quickly pass on details to their network operations teams.
- Detecting a problem at the feed handler does not tell you where the problem occurred. For instance, was it a problem with the Exchange or market data vendor's ticker plant, an internal network issue, third-party network carrier or extranet provider used to transfer the market data, firewall issue, or a problem in the end user's internal network?

All these questions lead to slow decision-making and long fault repair times that may take days to correct. Much of the technology used to monitor this infrastructure today is either not up to the task or involves expensive data capture, storage, and analytic technologies that have remained more or less the same for 20 years.

What is needed is an NPB that is designed to track real-time market data feeds. It instantly detects multicast sequence gaps and microbursts and can contain built-in decoders for high-performance monitoring of more than 300 financial exchange feeds. This delivers a low total cost of ownership while eliminating the need for expensive in-house multicast gap tools.

Improve Troubleshooting and Network Reliability

NETWORK VISIBILITY CAN BE USED TO REDUCE MTTR AND INCREASE NETWORK RELIABILITY

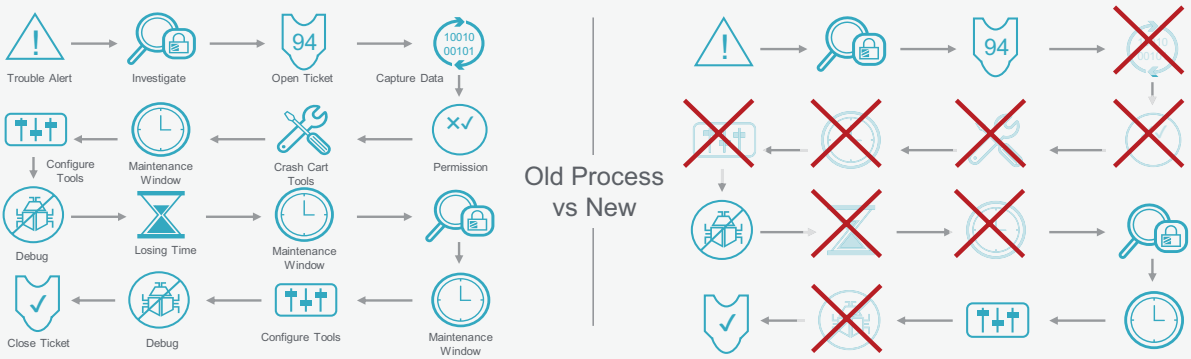
ixia
A Keysight Business

29 - REDUCE/ELIMINATE THE NEED FOR CHANGE BOARD APPROVALS AND CRASH CARTS

SOLUTION SUMMARY

- Once taps are inserted, no more network interruptions are needed for monitoring equipment
- An NPB is then connected after the tap for aggregation, filtering, and regeneration
- After tools are connected to the NPB, crash carts and many Change Board approvals are eliminated
- MTTR reductions of up to 80% are possible[28]

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Once visibility equipment is installed into the network, you rarely have to touch the network again. For instance, once a tap is installed, it is "set and forget" technology and will sit there passively forwarding a copy of all traffic to the NPB. Since the monitoring data is copied by the tap, you can do whatever you want because it will not affect the network. This has the huge benefit of eliminating most, if not all, Change Board approvals for troubleshooting purposes. You have already got the data access. If you combine that with a packet broker, you have got instant access to pretty much all the data you need across your whole network for troubleshooting. There is no need to wait two hours, two days, or two weeks for permission to touch the network.

This process reduction is shown in the image above. The left side shows a typical, basic process overview. An alert happens, you investigate it, open a ticket, ask for Change Board permission to touch the network, assemble the crash cart, wait for a maintenance window, then finally get some troubleshooting time in, you do not have enough time, do it all over, finally resolve the issue, and then close the ticket. On the right hand side, you can see where the effort was literally cut in half. Unless you are touching some mission critical component, you can skip Change Board approval and go straight to debugging—no crash cart or maintenance window needed. Authentication, authorization, and accounting (AAA) rules are typically preserved by the packet broker as well which further reduces the need for Change Board approvals. This new process has a big impact on reducing the mean time to repair. Case studies show that customers that can reduce their MTTR by up to 80%.[28]

30 - FLOATING FILTERS DRAMATICALLY CUT DATA COLLECTION TIMES

SOLUTION SUMMARY

- Pre-stage your filters and connect them to standby troubleshooting tools (e.g., analyzers, Wireshark)
- Use a drag-and-drop interface in the NPB to connect a network port to a filter
- Start capturing data in less than 1 minute and reduce troubleshooting costs

Deployment scenario: Out-of-band visibility architecture

SOLUTION OVERVIEW

Another troubleshooting example is to create unassigned data filters. These are called floating filters because they are not attached to a network port, so they are free floating. The power of the floating filter is that it is already created and connected on the tool side. When needed, the tools can instantly be connected to a network port to analyze incoming data. This speeds up diagnosis time since the forensic tools are already in standby mode.

When you are in a troubleshooting situation, minutes matter. According to the 2016 Cost of Data Center Outages study conducted by the Ponemon Institute, the average cost of a data center outage is $740,357 and lasts for about 95 minutes. This results in a cost of $7,790 per minute of downtime.[29] A rapid response is needed to control costs. Since the floating filter is already created, this can save you several minutes to more than an hour, especially when compared to configuring filters manually using command-line interface (CLI).

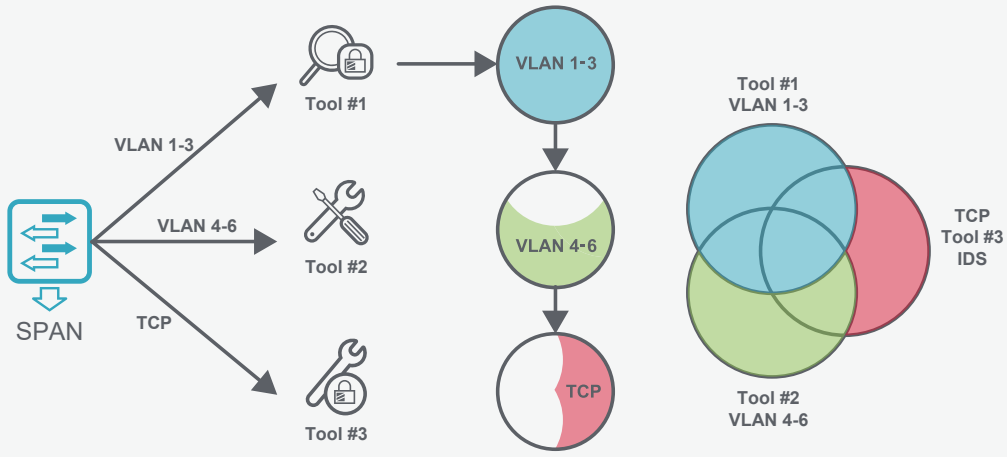
A typical use case would probably involve using a Wireshark tool or some sort of protocol analyzer. Any tool that is used often can be set up with a floating filter and pre-staged for problems. To activate the filter takes less than 1 minute. You simply draw a connection from the network port to the floating filter. It's that easy. If you need to make any filter adjustments, they are simple button clicks. In addition, the floating filters can be connected remotely by using the packet broker management system when needed. This gives you 24 x 7 x 365 diagnosis capabilities from remote locations.

31 - DYNAMIC FILTER ENGINES INCREASE DATA FILTER ACCURACY

SOLUTION SUMMARY

- 20% or more filters created through CLI have errors[30]
- Deploy an NPB that supports dynamic filtering to eliminate issues associated with CLI-based filters and guarantee accuracy
- Eliminate complexity and boost productivity up to four times that of a CLI process

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Traditional data filtering runs sequentially. During the process, each tool receives the data it needs, and then, the next tool downstream receives the rest of the data with any overlapping packets from previous tools missing (since that traffic was already claimed by tools earlier in the sequence). As you can see in the figure above, only the first tool in the sequence is guaranteed to receive all of the network traffic that it should be seeing. Subsequent tools may receive clipped data, or no data at all.

Dynamic filters are similar to that of ingress and egress filters except that the dynamic filter is located—and processed—in the middle, between the ingress and egress port filters. If dynamic filtering is used, the ingress filter can be left wide open so that the dynamic filters can segment and then aggregate packets from multiple ports and then send those packets on to the appropriate tool. This solution addresses problems that occur when some packets meet the filter criteria of multiple tools and must be sorted out properly for each tool to do its job. This is referred to as overlapping packets. While this problem is frequently overlooked, it must be addressed to ensure that your tools can "see" the right packets for successful monitoring.

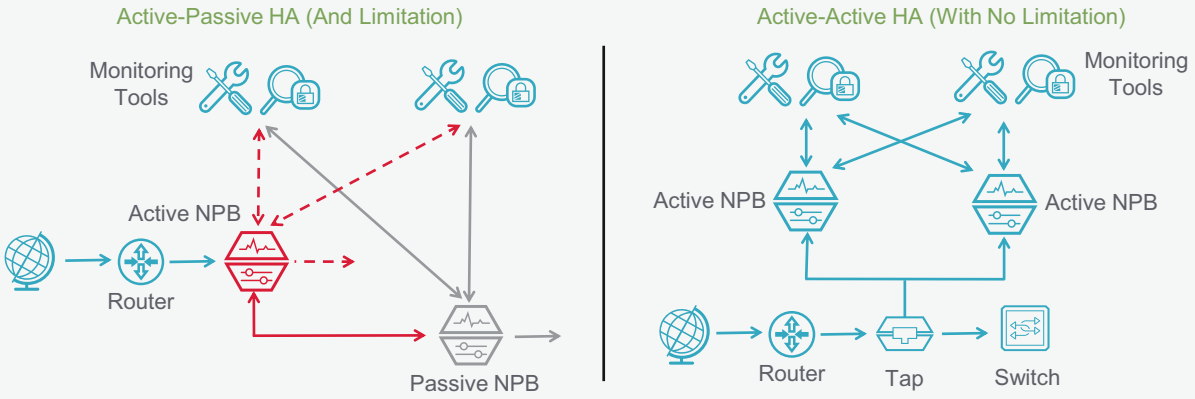
CLI-based filtering schemes put the onus of correcting this problem on the operator, requiring IT engineers to correctly identify any overlaps, quantify those overlaps, and then, write out detailed filter rules and exceptions to account for the data that needs to go to multiple destinations (tools). The dynamic filter eliminates the time and cost associated with CLI-based filters.

32 - IMPROVE OUT-OF-BAND MONITORING SOLUTION RELIABILITY WITH HA

SOLUTION SUMMARY

- The average cost of network downtime is $7,790 per minute[31]
- Use HA to create full redundancy (n+n) for out-of-band deployments of NPBs
- Heartbeat signals to tools enable super-fast fail-over between NPBs

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

This solution is an illustration of how you can increase reliability for your network monitoring solution by implementing survivability. There are two common options for survivability—full redundancy (typically with a primary and standby set of tools connected) and then what is commonly called an n+1 load balancing option (where you have all of the tools connected and functioning with some extra capacity). For the full redundancy option, this is highly effective at maintaining maximum network and tool up time. In terms of the network packet broker, this typically includes dual CPUs, dual power supplies, and fail-over between internal components. If one component, or path fails, the secondary equipment can handle the load. This option yields the highest level of MTBF.

How the HA solution is deployed is critical though. There are two options – Active-Active and Active-Passive. Active-Active means that both processors are working simultaneously to process traffic. Active-Passive means that only one of the processors is active while the second processor is in stand-by mode. Visibility solutions that are configured in active-passive mode will typically need a minute or more to restore full processing and restart data delivery. But a lot can happen in 60 seconds, and a lot of security issues can be missed. Redundant NPBs configured in active-active mode work with complete synchronicity to aggregate, filter, process, and deliver data to all security and monitoring solutions. This lets them work more efficiently, handle periodic traffic bursts, and failover in a few seconds or less to maintain continuous security inspection, without gaps.

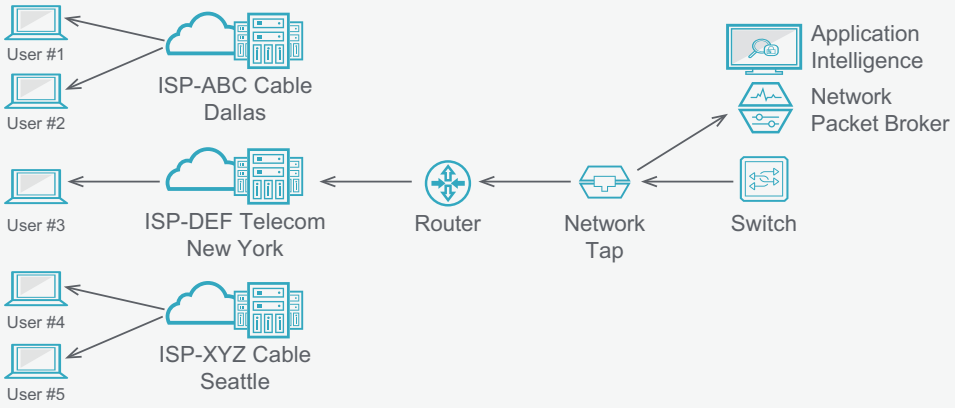
By using HA NPBs you can increase your network uptime and reliability far beyond the level provided with just redundant tools. And since you have a redundant NPB, maybe a redundant set of tools is no longer necessary.

33 - CONDUCT PROACTIVE TROUBLESHOOTING WITH APPLICATION INTELLIGENCE

SOLUTION SUMMARY

- Most IT teams spend around 36% of their daily efforts on reactive troubleshooting[32]
- 85% of MTTR is spent trying to figure out that there is indeed a problem[33]
- Use of an NPB with detailed user geolocation, BGP AS, and application traffic changes can help pinpoint problems

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

According to the EMA Network Management Megatrends 2016 report, network teams spend 36% of their time on reactive troubleshooting.[32] This means less time on value-added projects. In addition, research from analyst Zeus Kerravala shows that up to 85% of the time associated with network mean time to repair is simply spent trying to figure out that there is actually a problem.[33] So, identifying a common denominator among the people having a problem can be important to minimizing outage durations. The key is to investigate rich metadata, which can provide a lot of context about the user's connections to help you quickly isolate issues. With the NPB, you can filter data based upon: application signature (and granular application actions), application bandwidth consumed, geographic location information, browser types in use, and device types in use.

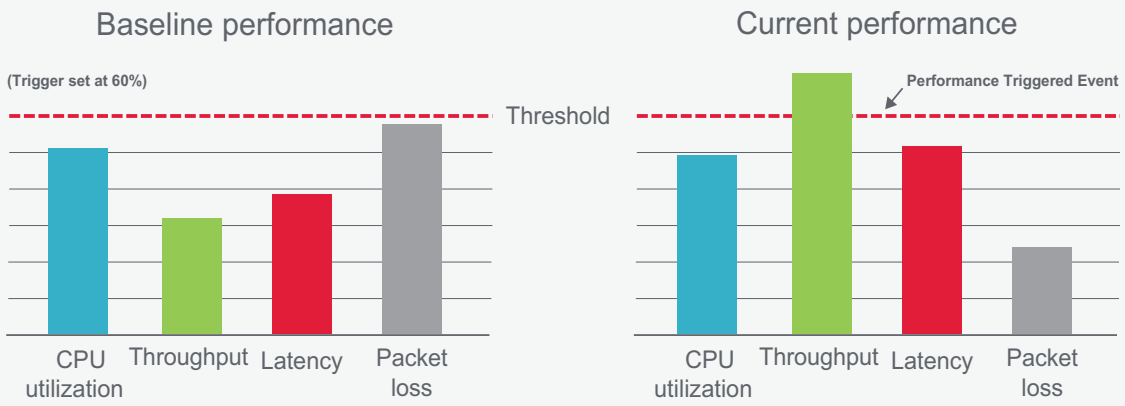
Here is an example. A user calls in to the technical assistance center to report that their online gaming service does not work today. The gaming company representative looks at their servers and equipment, but everything is okay. The gaming company also has not received any widespread complaints in the last 48 hours. The next step is to start troubleshooting with the individual. The technician resets the customer account data, but nothing happens. Next, the technician spends lots of time trying to figure out what the problem is. In the meantime, this issue is happening for several customers, but it is still not a widespread issue. By using available application data, the gaming company network operations center (NOC) could quickly have seen that there were multiple complaints from one geographic area and narrowed it down to one Internet service provider (ISP) (ABC cable company). Then the gaming company could have called that one ISP and found out that they performed a software update during the night. This update will end up being the source of the problem that needs to get troubleshot—not the individual customers.

34 - BASELINE YOUR NETWORK TO RECOGNIZE ABERRANT BEHAVIOR

SOLUTION SUMMARY

- The average duration of a data center outage is 95 minutes[34]
- Characterize your network to create a baseline of the different network that can be used to recognize aberrant behavior[35] by using taps and NPBs to capture pertinent data
- Create a "golden configuration" for comparison when performing upgrades and rollouts

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

When talking about network monitoring, one of the first things that comes to mind for most people is the ability to capture network data and troubleshoot problems or increase performance. However, one of the most important reasons to implement network monitoring is to characterize your network. How does it perform normally? What is the throughput, bandwidth consumed, size and location of data flows, and average delays caused by data inspection (for security purposes)? Before you can do anything else, you need this baseline of your network. Once you have the baseline, you have something to compare to and you will be able to recognize aberrant behavior and normal behavior.

This is where a visibility architecture will help. Through a controlled plan (data access, monitoring control layer, and security and monitoring data analysis), you can create the baseline for the different layers of your network like:

- Internal data network
- Data storage network
- External facing components (website, ecommerce, channel partner portals, etc.)
- Virtual data center
- Security architecture
- Network management systems (NMS, orchestration, capacity planning, etc.).

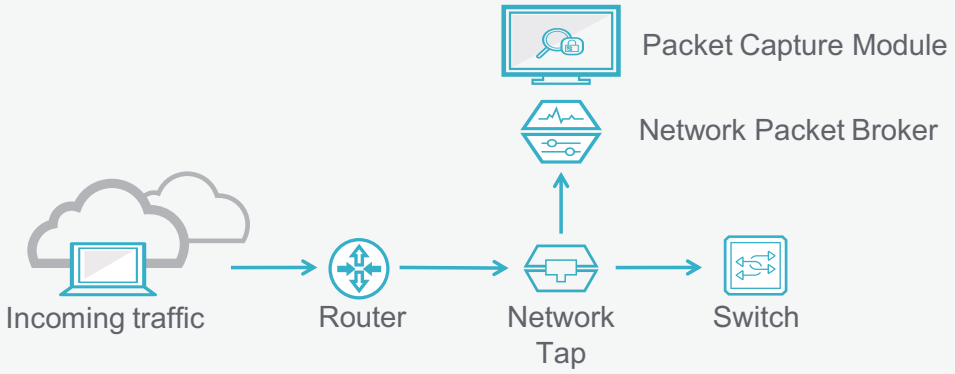
Taps and NPBs are the first starting point to collect the required data. This data can then be filtered and distributed to analysis tools like a network performance management (NPM), application performance management (APM), DLP, or proactive monitoring solution that can be used for deep analysis and document normal parameters. This is then used as the "golden configuration" for future performance and network behavior analysis.

35 - IMPROVE TROUBLESHOOTING WITH QUICK PACKET CAPTURES

SOLUTION SUMMARY

- Quick data captures make troubleshooting activities more convenient
- Use an NPB to capture a range of packets (up to 14 GB) at line rate up to 40 Gbps
- Packet captures can then be quickly decoded with an on-board analyzer

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

An NPB can be used to create quick and easy packet captures (PCAPs) of network data. An onboard analyzer allows for quick decode of the packet data. This solution allows IT staff to have an integrated, single-UI capture and decode capability to quickly solve point problems.

Packet capture capability can be conducted at rates up to a 40 Gbps line rate. The simplicity is created by enabling the capability through the drag-and-drop GUI interface to create either manually initiated, event triggered, or API initiated packet captures. This means that the engineer does not need to flip back and forth between applications. An extensive list of trigger fields (media access control (MAC) address, VLAN, Ethernet type, IP address, MPLS label, IP Protocol, Transmission Control Protocol (TCP) control, or Layer 4 port) makes the solution even more powerful.

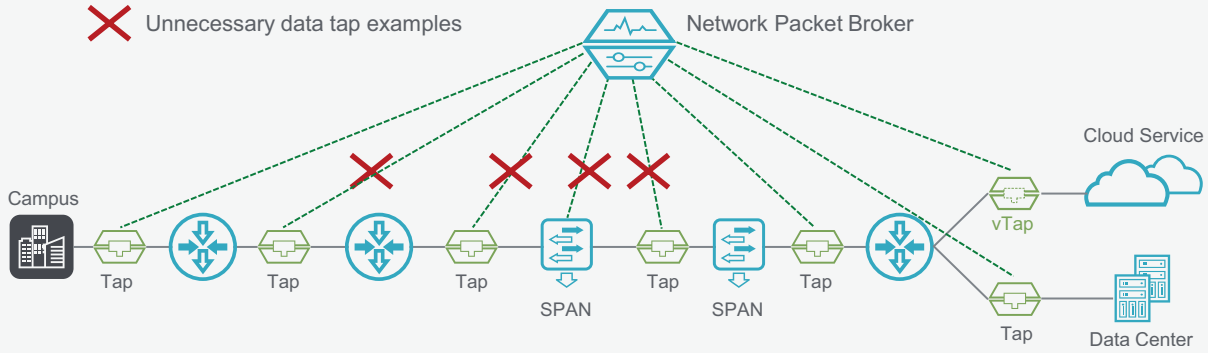
A key component to realizing maximum value from the solution is to utilize the buffered window to catch pre-event packets. This allows you to capture data before and after the trigger event. A sliding capture window and the ability for on-board and off-board storage provides more utility.

36 - USE DUPLICATE PACKETS TO ISOLATE ARCHITECTURE DESIGN FLAWS

SOLUTION SUMMARY

- As much as 50% of network monitoring traffic can be duplicate data[36]
- Temporarily turn deduplication off in the NPB when debugging to expose hidden architecture issues
- Measure amount of inherent duplicate packets on the network and compare to the previous baseline

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

While duplicate packets are generally thought of as bad, they can have a positive benefit. This is because their existence can be an indicator of several network issues that should be addressed. Some examples include malfunctioning hardware devices, a flaw in your visibility architecture that is resulting in the creation of too many copies of the same information, the design of your Cisco ACI architecture or a flaw or malfunction in your data filtering device (SPAN session programming, network packet broker, etc.) for network monitoring data. So, the existence of duplicate packets may not be all bad.

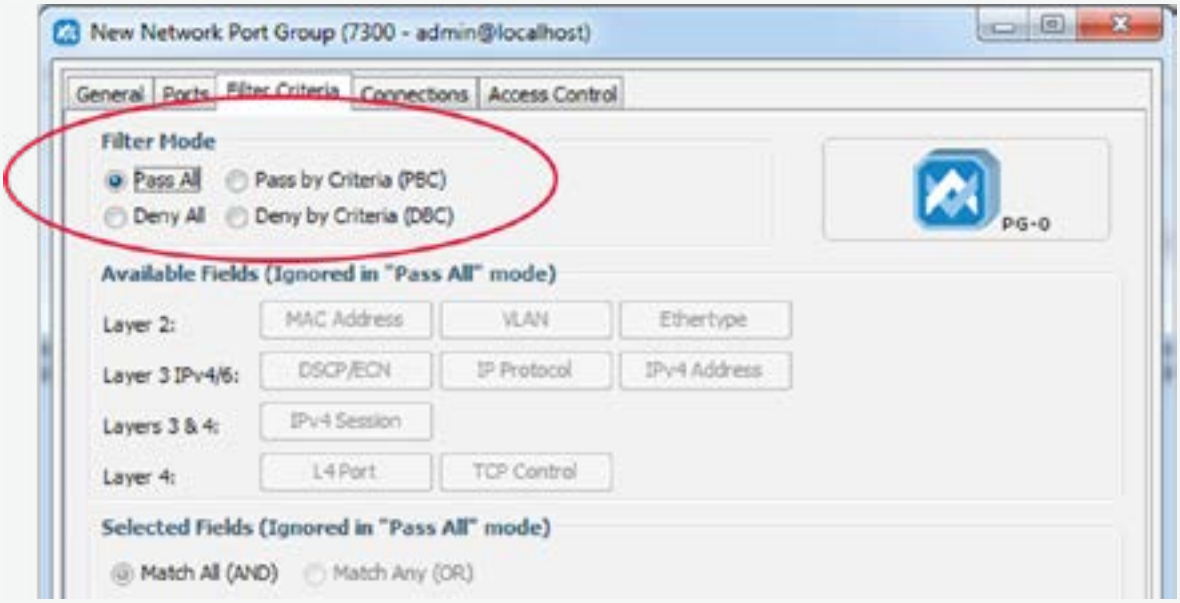
As an example, a well-designed packet broker has the ability to turn deduplication capabilities on and off. By turning deduplication capabilities off periodically for troubleshooting purposes, an IT engineer has the ability to observe the amount of duplicate monitoring data on the network and compare to previous baselines. This allows you to find: duplicate data access points, duplicate route paths, access burden issues, broken equipment, etc. With the new knowledge, you can then make any adjustments to the network or reprogram any of the data filters.

37 - EASILY VALIDATE YOUR MONITORING FILTER ACCURACY

SOLUTION SUMMARY

- 20% or more filters created through CLI have errors[37]
- Reduce filter validation time from an hour to 5 minutes
- NPBs have a simple button click that changes the “pass by” criteria to “deny by” to validate that the monitoring data filters are working correctly

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

A well-designed NPB can be used to quickly validate the filters that it creates. While some solutions, especially SPAN port filters, require extensive external tool setups to validate data output, an NPB can use an internal setting for validation.

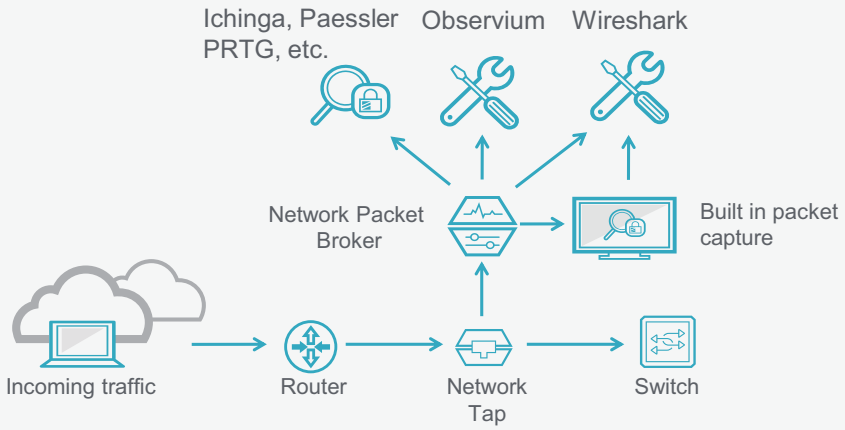
In the NPB graphical user interface (GUI), once a filter is created to allow only certain types of data to pass by, save the filter. After that, go back into the filter and flip the “pass by” criteria to “deny by” criteria to see if the intended data is actually being filtered out correctly. This simple setting gives you the inverse of what you wanted. If the data sent out of the NPB contains some of the data you are looking for, then you know that one or more parameters within the NPB filter were set wrong. Since you can see the data output at your tool, you should be able to easily modify your data filter to correct the problem. This can reduce the filter validation process to only a few minutes, versus other validation mechanisms that could take more than an hour.

38 - IMPROVE NETWORK RELIABILITY ANALYSIS WITH BETTER MONITORING DATA

SOLUTION SUMMARY

- Use taps to reliably capture data for tool analysis
- Use an NPB to capture and filter data to specific network reliability monitoring tools
- Use an NPB with packet capture capability to generate and analyze PCAPs

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

An NPB can be used to correlate the necessary data used to help improve network reliability. While this is similar to network performance monitoring (which typically uses purpose-built tools in that area), it is not the same. Network reliability monitoring is more focused upon network uptime, network availability, the amount of performance impairments discovered, time to resolution statistics, etc. Network reliability can also get very specific to the network depending upon usage, for instance, whether most of the server access is from internal or external sources (like ecommerce).

In this use case, the NPB is used to filter and serve data to various tools as part of this solution. Selected data is filtered within the NPB and then distributed to one or more tools. This can include tools like Cacti (used to monitor and graph ping times and server events), Icinga (the modern version of Nagios used to measure various reliability parameters like network uptime), Paessler's PRTG (used to measure uptime), Observium (used for trending analysis), and various other tools and dashboards to collect and present the data.

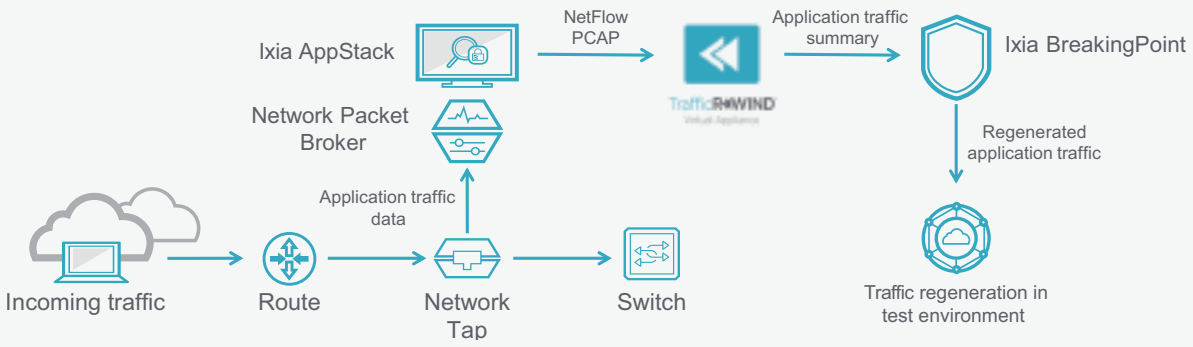
Taps and NPBs can be used for operational and administrative segmentation of the monitoring network to separate the visibility architecture (including the tools needed) from the general network. Packet Captures (PCAPs) can also be generated by the NPB and analyzed with reliability tools to gather more network information. Once the segment is created and data collected, it can be used for the reliability solution analysis, which typically consists of creating regular baselines of data criteria performance, analysis of flow data, trending of criteria performance, and observations of remediation successes/failures.

39 - CORRELATE PRODUCTION TRAFFIC WITH TEST ENVIRONMENTS TO REDUCE MTTR

SOLUTION SUMMARY

- Save an average of 21 hours of downtime per year[38] with application level PCAP analysis
- Record network traffic dynamics including application type, bandwidth distribution, and application behavior using NetFlow information
- Reproduce the realism of production networks in the lab

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Ixia has created a unique solution called TrafficREWIND which combines Ixia's visibility and test expertise to improve fault analysis and also validate architectures and devices before deployment. TrafficREWIND translates production network insight from the AppStack application intelligence product into test traffic configurations. The resulting configuration can be used by the BreakingPoint application and security test solution to better analyze network security threats.

TrafficREWIND is a virtual appliance that can be easily deployed anywhere in any production network. It offers a scalable real-time architecture to record and synthesize traffic characteristics over extended periods of time (up to 7 days), without legal- or compliance-related concerns in recording or sharing actual data payloads. This allows not only replicating the traffic profile with the associated real-world applications, but also adds an unprecedented test dimension of dynamically changing traffic composition over time to model the temporal nature of networks and applications. AppStack leverages IxFlow, Ixia's unique set of NetFlow extensions, to feed application-level insights into TrafficREWIND. This rich NetFlow metadata includes a wide array of network activities along with application and device behavior seen in production networks. This creates a solution that can improve fault analysis or be used to validate architectures and devices before deployment. The network insight captured in AppStack metadata bolsters the BreakingPoint solution with traffic realism.

Enterprises, service providers, and network equipment manufacturers (NEMs) waste valuable time and resources trying to replicate production network traffic conditions for fault analysis or to validate architectures and devices before deployment. Based on a Veeam Report,[39] the average enterprise experiences almost 13 incidences of application downtime per year that costs an average of $10,163,114 annually. Assuming an improvement of the MTTR by even 25%, TrafficREWIND`s approach combined with the BreakingPoint test solution could save companies over 21 hours of downtime per year.[38]

Remove Network Blind Spots

REMOVE BLIND SPOTS TO REDUCE NETWORK ISSUES, SECURITY RISK, AND COMPLIANCE ISSUES

ixia
A Keysight Business

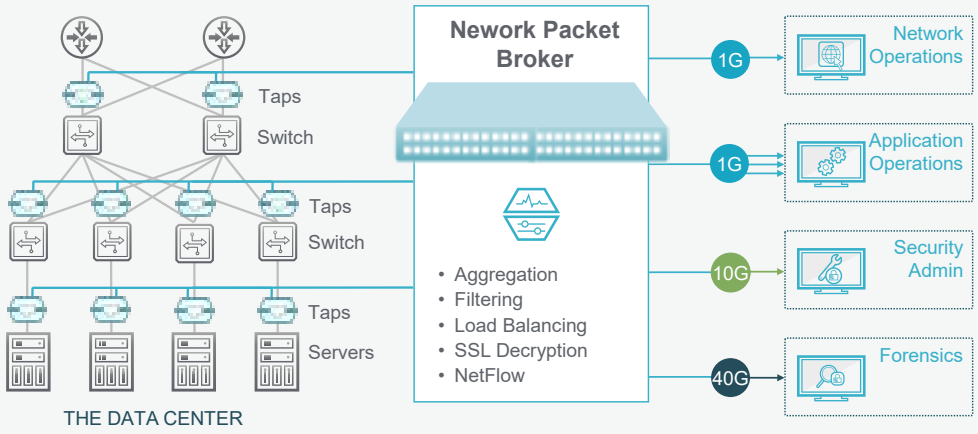
915-8138-01-9081 Rev B

40 - VISIBILITY ARCHITECTURES EXPOSE MISSING/HIDDEN DATA

SOLUTION SUMMARY

- Security and monitoring tools are only as good as the data they are seeing
- SPANs drop important troubleshooting data (malformed and missing packets)
- 20% of data filters configured through CLI are wrong and clip data[40]
- By deploying a Visibility Architecture you can reduce/eliminate these blind spots

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Most engineers assume that the data they collect is correct. What if it is not? How would you know? The simple fact for most IT departments is that you will not know. This is one reason why security breaches occur and last as long as they do. According to the 2016 Verizon DBIR[41], almost 75% of companies that were breached had to be told by someone else—law enforcement, customers, or business partners. Those victimized companies had no idea themselves about the breach. Other data from the Ponemon Institute's 2015 Cost of Cyber Crime Study showed that it is actually taking businesses longer to resolve cyber-attacks.[42]

Another issue is SPAN ports. For out-of-band monitoring situations, if you are not using taps, then SPAN ports will only give you summarized data—not the full data. This means that critical (bad) data right before an incident happens is probably omitted from the SPAN data, and you may not have the data you need to accurately diagnose the source of a problem/attack. SPANs also have the lowest priority for data switching functionality. Therefore, if the switch is running at full processor capability (due to a distributed denial of service (DDOS) attack or something), packets on the mirroring port can get dropped and you will miss critical data.

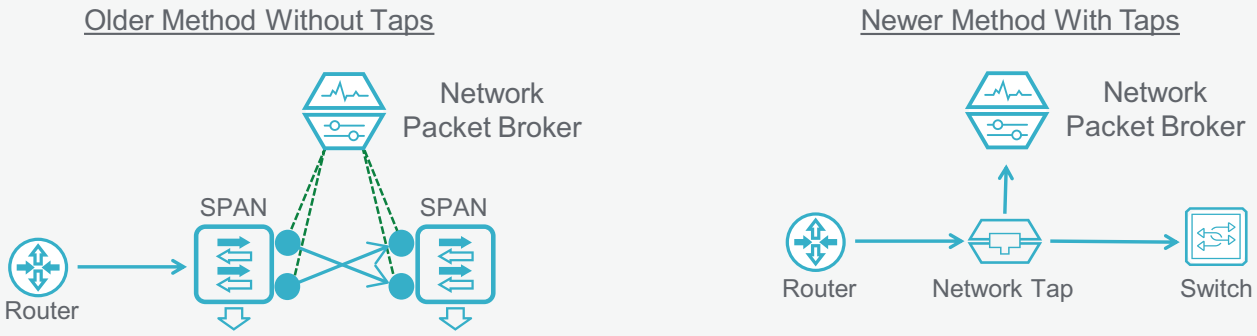
A third issue is the integrity of the data filters. Using CLI to program SPAN ports or packet broker filters is a very common way of creating errors. CLI provides lots of ways to make a mistake, either through syntax errors or filters being used to provide multiple copies of data to different tools that end up overlapping each other and dropping vital data. In fact, approximately 20% of the time that CLI is used to create monitoring filter—it ends up being wrong, i.e., the command line interface approach results in some sort of programming error.[40] Creation of a visibility architecture eliminates these, and other, network blind spots.

41 - TAP DEPLOYMENTS IMPROVE DATA COLLECTION

SOLUTION SUMMARY

- For network monitoring, ensuring proper access to network data is the most critical thing you can do
- Taps are “set and forget” technology
- 78% of organizations deploy taps across 50% or more of their network[43]

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

When it comes to data monitoring, ensuring proper access to network data is the most critical thing you can do. Everything else, data filtering and the conversion of data into actionable information, are all dependent on that initial data being correct and relevant. Enterprises require 100% visibility into network traffic to ensure peak performance and security. As the network grows larger, visibility becomes harder and blind spots creep into the network. These blind spots, or the inability to completely see what is happening on the network, can compromise network quality.

Network taps (test access points) are a key part of the access layer of a visibility architecture, because they are an unobtrusive way to capture monitoring data. The access layer framework of a visibility architecture is focused on creating access to the business data information within the network. This is the base framework that then feeds data to NPBs, where it can be filtered before being be sent on to the appropriate monitoring tools.

Network taps are most commonly used in physical networks to copy network data and forward a copy of that data to monitoring and security tools. While the tap is installed directly into the network, it is a one-time disruption to the network. After that, the tap is designed to have passive functionality. This prevents the monitoring infrastructure from impacting network availability.

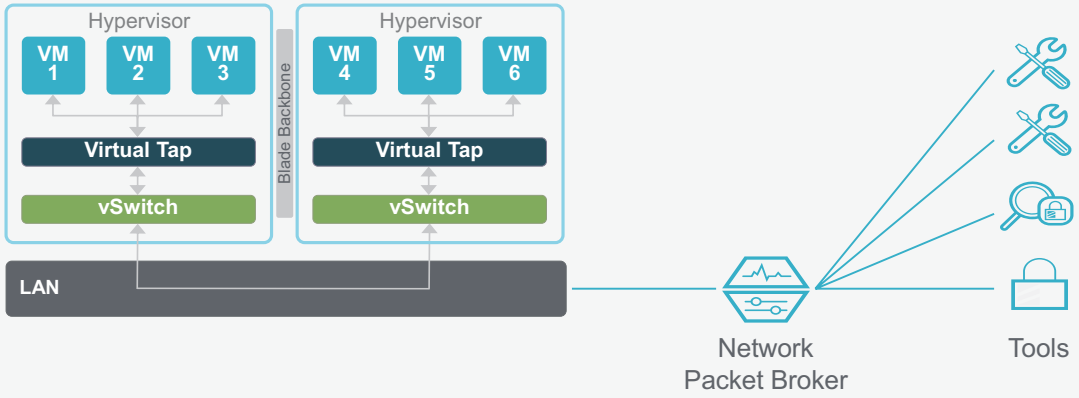
This type of tap provides permanent access to network traffic and allows total traffic visibility for network monitoring and security devices—without introducing costly bottlenecks or points of failure. In addition, taps are plug-and-play and do not require any costly hands-on management. They can be installed anywhere in the network, regardless of interface or network location. You simply match an appropriate tap up to the: cabling type (e.g., copper, multimode fiber, or single-mode fiber), maximum network speed required (e.g. 1/10/40/100 Gbps), and the desired split ratio (e.g., 50/50, 60/40, 70/30, 80/20, or 90/10) needed for your transmission distances.

42 - VIRTUAL TAPS EXPOSE HIDDEN EAST-WEST TRAFFIC IN VIRTUAL DATA CENTERS

SOLUTION SUMMARY

- Two-thirds of enterprises use virtualization for business critical applications but over one-third are concerned about their ability to monitor it[44]
- Up to 86% of virtual data is east-west and never reaches the top of the rack[45]
- Some VM mirroring solutions can only make a complete copy of the data which overloads the LAN
- A virtual tap with built-in pre-filtering eliminates these problems

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

While virtual data centers and virtualization technology have significant cost benefits, they can pose a significant hurdle to network visibility. Ixia research from a 2015 survey report shows that two-thirds of those surveyed use virtualization technology for business critical applications.[44] At the same time, over one-third are concerned about their ability, or lack thereof, to monitor virtual technology. Part of this is simply due to data access. According to Cisco Systems research information, up to 86% of virtual data center traffic will travel in an east-west direction by 2020.[45] This means that this type of traffic never reaches the top of the rack where it can be captured by a traditional physical tap or SPAN. So, you literally have no idea what is, or could be, passing back and forth on your virtual machines.

This could lead to security, performance, and regulatory compliance infractions. For instance, there are malware variants, like Crisis, that have been optimized for virtual data center environments. How do you know you do not have a security issue in your virtual data center? You will know when it is too late. The same thing with performance. By the time you see a performance problem, it is probably going to be too late—internal and external customers are probably going to notice it first.

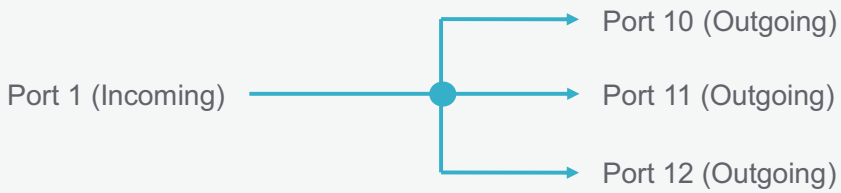
What you need is access to that virtual stream of data so you can send selected copies of it to your monitoring tools for analysis. Virtual taps can remediate this blind spot. A virtual tap is software that behaves like a physical tap. You load the software into a VM. It then makes a copy of all inter- and intra-VM traffic on VMware, Hyper-V, and KVM systems. Once you have a copy of the data, a good virtual tap gives you a way to perform some basic filtering of that data and then export it out to a physical packet broker where you can filter the data and send it on to your existing tools for analysis.

43 - REGENERATE MONITORING DATA FOR DISTRIBUTION TO MULTIPLE DESTINATIONS

SOLUTION SUMMARY

- Security and monitoring tool deployments continue to grow 10 to 15% per year[46]
- Regenerate the same traffic flows to multiple tools simultaneously for parallel purposes
- Use an NPB for data regeneration to simplify your monitoring architecture and reduce costs

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Most businesses have multiple tools these days. A recent EMA survey states that the average enterprise has between 4 and 15 types of security and monitoring tools.[46] This is an increase of 25 to 30% over the previous 2 years. All of these tools need data and many need subsets of the same kind of data. This is where an NPB can provide a valuable service.

An NPB can be used to aggregate monitoring data from multiple sources, generate multiple simultaneous copies of that information, and then transmit that data to various security and monitoring tools for analysis. The network traffic is regenerated in real-time at line rate. This means the simultaneous distribution of data to multiple egress ports. When this is combined with dynamic filtering, the data transmitted to the egress port can be further filtered to pass the precise set of information to the tool connected to that port.

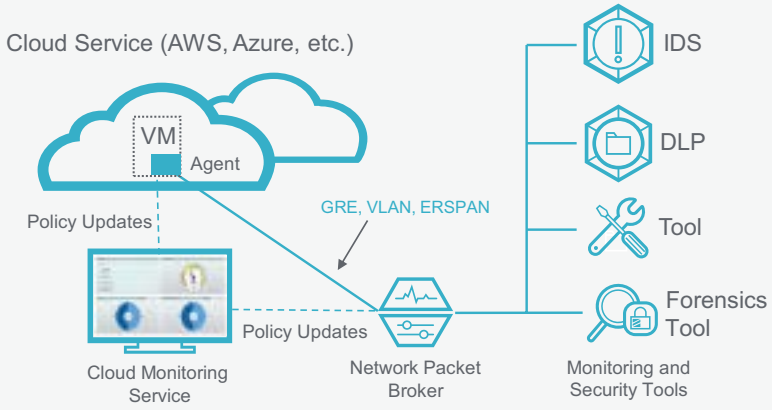
As an example, suppose there is interesting information on VLAN 101. That information may need to be sent to three tools (a DLP, a recorder, and a compliance tool). An exact copy of the data is created and sent to three appropriate egress ports on the NPB for transmission to the respective tools. However, maybe the DLP does not need a copy of all of the information, it only needs traffic to certain IP addresses or only email traffic. The non-interesting traffic is dropped at the egress port, and the required traffic is then sent to the DLP for analysis. Without an NPB, three separate taps would have been needed for that segment to connect the data to the three tools. There also would not have been any filtering and the flexibility of the solution is limited, as each tap would be dedicated to a tool. Unnecessary costs would then be incurred, which would offset the cost of the NPB purchase.

44 - ACQUIRE VISIBILITY INTO CLOUD NETWORKS

SOLUTION SUMMARY

- The average enterprise uses six different cloud networks[47]
- Traditional monitoring solutions do not work in public cloud networks
- Use a cloud monitoring solution to capture monitoring data and distribute the data to physical or virtual tools

Deployment scenario: Cloud visibility architecture



SOLUTION OVERVIEW

Cloud networks have been touted as a panacea for businesses, because they allow you to spin up network functionality extremely fast. Unfortunately, these networks have extremely poor visibility into areas of performance, security threats, and compliance initiatives. Traditional monitoring tactics like taps, NPBs, and physical security and monitoring tools are ineffective for this new architecture because of the lack of access to monitoring data. A cloud-based solution is needed to solve the access problem and gives you the ability to see the data you need.

Ixia's solution is a software as a service (SaaS) solution. In essence, it is a collection of Amazon Web Services (AWS) that support cloud agility with a server-less design. The basic design includes three components: source sensors (agents) installed in the network that collect and filter cloud data, tool sensors (agents) that are installed on the virtual network tools and deliver the requisite monitoring data to that tool, and a management system that lets you remotely configure and control the different agents. The agents are installed as Docker containers on the source and tool instances.

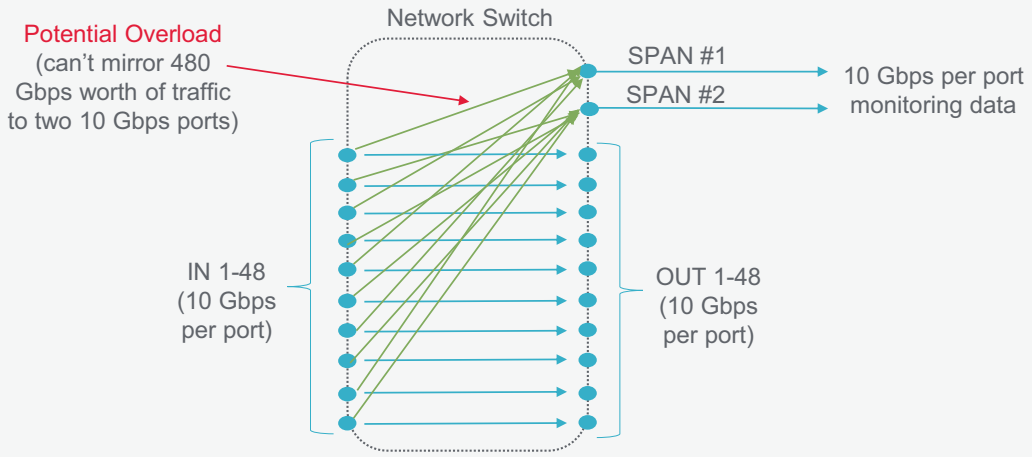
Monitoring data from the agents include: underlying instance architecture, operating system information, hypervisor type, kernel and software versions, prepopulated user data, CPU and memory utilization, and performance metrics. This gives you the access to the cloud data that you need and delivers the information right to your analysis tools.

45 - ELIMINATE DATA OVERLOADING OF NETWORK SWITCH SPAN PORTS

SOLUTION SUMMARY

- SPAN ports can drop data without any notification of the data loss
- Eliminate a common source of network blind spots due to missing data
- Use a tap and NPB to decrease MTTR with better network visibility

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

A SPAN port, also called a mirroring port, is a special port on a network switch that is used to create a copy of specific network data. This copy can then be sent to monitoring tools for analysis. One major issue with that type of solution is that while the SPAN port has a buffer, the buffer is not infinite. It can become overloaded and drop data, especially since there are typically only two dedicated SPAN ports on a network switch. This also creates a SPAN port contention issue mentioned earlier.

Since the data travelling through the switch is often far more data than what can be transmitted out of the SPAN ports, this means that data can, and will, be lost. What is worse, data (like bad checksum packets, malformed packets, too big or small packets, etc.) can be dropped even if there is no load. The same is true for VLAN access control lists (VACLs) which are specialized ports on Cisco Catalyst switches for VLAN data. In addition, when the switch CPU is overloaded, the switch will drop monitoring data on the SPAN ports as the SPAN port is a low priority resource.

The solution is to use taps for data capture and an NPB to filter the data to completely eliminate the SPAN port overloading issue and the data loss issue. Taps and the NPBs can run at full line rate and provide a very cost-effective solution.

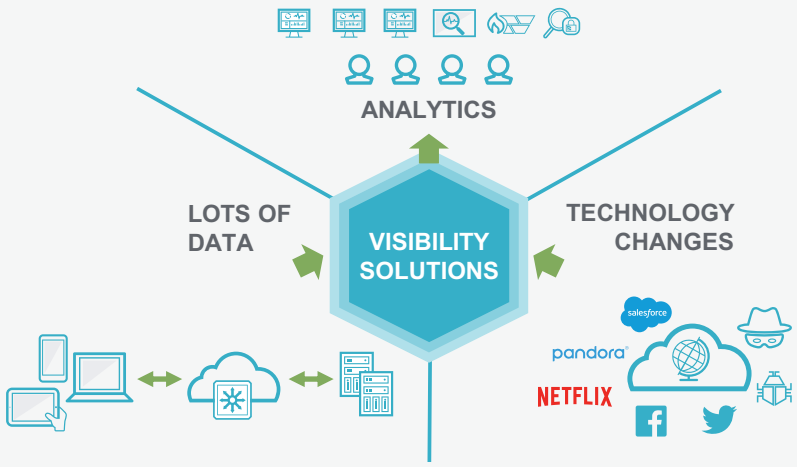
An Ixia case study shows the various problems that a national pharmacy ran into with SPAN ports that were dropping packets and creating a loss of information due to a data overload condition.[48]

46 - REDUCE NETWORK COMPLEXITY WITH VISIBILITY ARCHITECTURES

SOLUTION SUMMARY

- Every 25% increase in functionality of a system creates a 100% increase in complexity[49]
- Global IP traffic is expected to triple from 72.5 EB per month in 2015 to 194.4 EB per month in 2020[50]
- Use a Visibility Architecture to reduce complexity by sending tools only the information they need

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

As businesses deploy more technology to solve problems, complexity becomes inevitable. The rate of increase of this complexity has been characterized by David Cappuccio who stated at a Gartner Symposium back in late 2012 that, for every 25% increase in functionality of a system, there is a 100% increase in complexity. A blog that Eric Savitz (with Forbes) wrote has more information. In any case, that was back in 2012.4[9] One can only imagine that the ratio has gotten worse over the last several years with the proliferation of BYOD, cloud everything, and the Internet of Everything.

Typically, there are four fundamental sources of complexity—the network, new equipment, monitoring tools used, and the network architectures being used. Network complexity is created when new links and office locations are added. They can be set up with different VLANs, sub-nets, etc. to geographically segment them. These segmented networks often have separate equipment that is used for remote logon, authentication, and other activities which makes it hard to track what is happening at those locations. There are also BYOD and Wi-Fi access issues to contend with. The situation will only get worse, especially due to data overload. A Cisco report states that global IP traffic is expected to triple from 72.5 Exabytes (EB) per month in 2015 to 194.4 EB per month in 2020.[50]

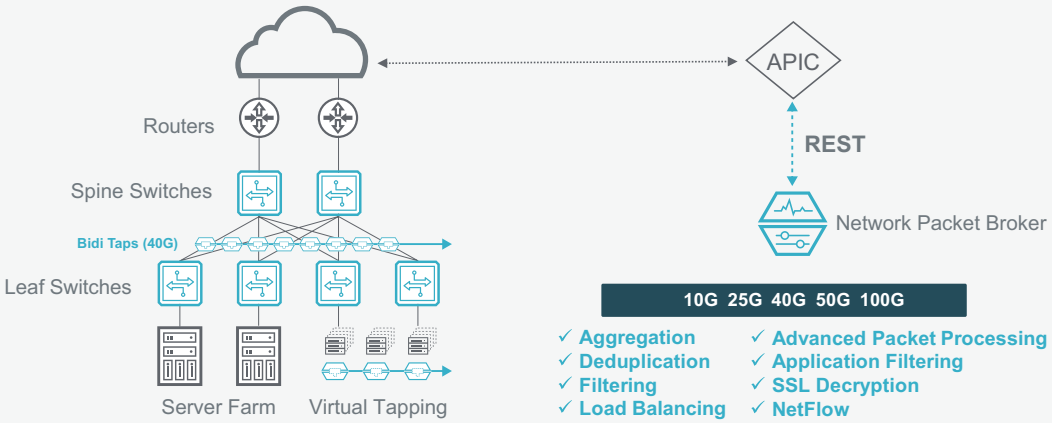
However, complexity does not have to be unmanageable. As mentioned earlier on, the purpose of a visibility architecture is to plan out your monitoring strategy. For instance, how does it tie into your various tools like an IPS, IDS, DLP, SIEM, data recorder, protocol analyzer, etc? A visibility architecture and NPB's allow you to create an architecture, gain access to VLANs and subnets, and allows you to manage the data and tool overload situation. Discrete data, or data types, can be captured and sent to a single or multiple tools for analysis. This creates the requisite visibility into network and security architectures.

47 - MONITOR CISCO ACI SWITCHING AND MIRRORING SOLUTIONS WITH EASE

SOLUTION SUMMARY

- Improve ACI deployments with advanced Layer 2 through 4 filtering, application filtering, SSL decryption, load balancing, data masking, and header stripping/packet slicing
- Eliminate ERSPAN encapsulation-related issues and strip VXLAN headers
- Offload NetFlow/IPFIX traffic generation issues for switches

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Cisco has created various technologies for its network infrastructure. This includes mirroring technologies for packet and flow data like: SPAN, Remote SPAN (RSPAN), Encapsulated RSPAN (ERSPAN), VLAN access control list (VACL), and NetFlow. SPAN ports have various issues—see the separate solution brief on this.[51] SPAN related technologies like RSPAN and ERSPAN also have concerns associated with them, especially for large enterprises and carriers. For instance, ERSPAN uses GRE encapsulated data which typically needs to be decapsulated before transmission to monitoring tools. An NPB is typically needed to perform the GRE decapsulation and stripping it off before transmission to the tools. In addition, ERSPAN does not support fragmented frames and jumbo frames, which often have issues with network propagation, since they extend beyond the 1500 byte maximum transmission unit (MTU) limit (due to the 50 byte encapsulation protocol). VLAN access lists (VACLs) tried to improve some of the SPAN limitations with some basic filtering (like TCP port and IP addresses), removing the two port limitation.

An emerging Cisco technology, Application Centric Infrastructure (ACI), focuses on distributed applications. It uses a centralized controller and an overlay structure to create, deliver, and automate application policies throughout the network. However, issues like duplicate packets and the need for advanced filtering capabilities still exist. SSL-encrypted data issues are often a problem for tools as well.

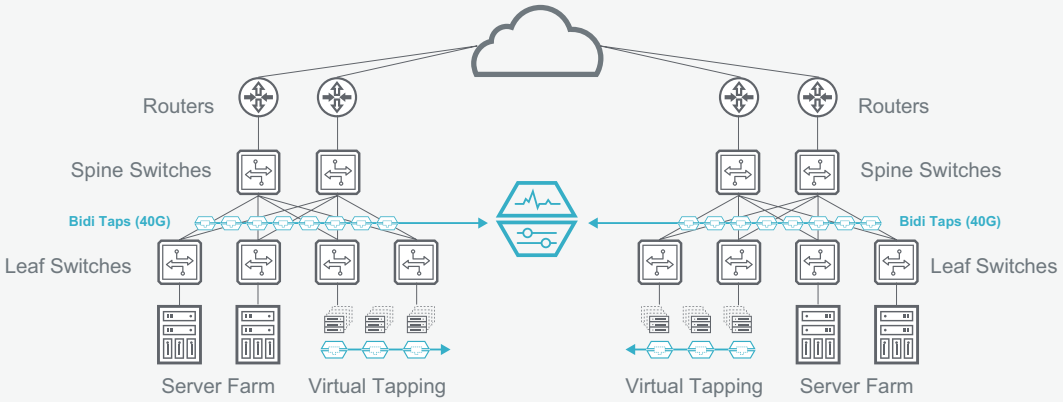
VXLAN headers are often used to create the ACI network overlays. Unfortunately, many monitoring tools do not understand the VXLAN headers, so they will need to be removed from the monitoring data by an NPB before the data can be sent to the tool(s).

48 - OVERCOME VISIBILITY LOSS DUE TO M&A NETWORK INTEGRATIONS

SOLUTION SUMMARY:

- In 2016 there were approximately 48,825 worldwide mergers and acquisitions[52]
- Overcome network integration issues associated with company mergers
- A visibility architecture can be used to bridge disparate networks and equipment

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Today's business environment can create serious headaches and security risks for IT. Mergers and acquisitions are common occurrences. In 2016, there were approximately 48,825 worldwide mergers and acquisitions (M&As).[52] Incomplete and/or poorly executed IT integration projects are commonplace as well. McKinsey & Company found in one of its studies that 56% of IT projects deliver less value than expected, and 17% failed so badly that they threatened the existence of the company.[53]

These situations, especially M&A's, can create a blending of disparate equipment and systems that often result in very limited network visibility, i.e., blind spots, and increased security risks. This is because the networks do not pass along information well, so no one really knows what is happening. In addition to there simply just being different types of applications in use across both networks (enterprise resource planning (ERP), NMS, customer relationship management (CRM), etc.), there can be different security architectures and policy management in use. For instance, one network could be using A10 decryption devices and Cisco SourceFire IPSs while the second network could be using BlueCoat decryption devices and FireEye devices. There may also be different APM and NPM tools. This situation creates various interoperability issues including: system/application downtime, system capabilities being turned off to improve network performance, and the scaling back/elimination of network and application monitoring while extensive network re-architecting takes place.

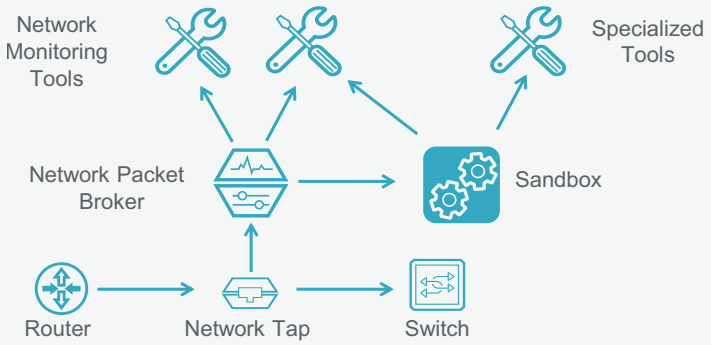
The short- and long-term solution is to implement a visibility architecture. Use taps to access network data where and when you need it. After that, packet brokers can be used to aggregate the data, prevent tool overload due to different network data speeds, filter uninteresting data, and then distribute the data to the appropriate tools. This gives IT back its control, as it can get a complete picture across the network to investigate any network issues, bandwidth issues, application performance and availability issues, properly localize problems, and get access to the data they need, when they need it. In addition, bypass switches and inline NPBs can be used to increase network reliability and uptime.

49 - IMPROVE SANDBOXING EXERCISES TO VALIDATE NETWORK DESIGNS

SOLUTION SUMMARY

- A sandbox is an isolated computing environment in which a program or file can be executed without affecting the application in which it runs[54]
- Test new equipment and monitoring tools before a rollout to ensure success
- Use a visibility architecture with NPBs to create a cost-effective sandbox

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

A sandbox is one way that network and security architects can test new equipment and processes. This is a purpose-built area that is walled off from the main corporate network, but it should mimic the production environment to give a realistic experience. This allows IT engineers to practice and test deployments for effectiveness and complexity before a general rollout.

A properly designed sandbox should include a visibility architecture with taps, bypass switches, and NPBs that can be used to capture network data and direct that data to specific tools for analysis. For instance, maybe you need a protocol analyzer, NPM, APM, or some other tool to validate the new equipment and/or configuration. Maybe multiple tools are involved. The NPB lets you capture and filter specific monitoring data that can then feed all of your analysis tools. In fact, you might be testing a new security and monitoring tool before rollout to the production network and want to see how well it will work. The sandbox is a perfect place to find out.

Many sandboxes are simply applications running on VMs. If this is the case, a virtual tap can be used to capture the requisite data and forward it to an NPB for distribution to the monitoring tools.

Optimize Network Performance

VISIBILITY SOLUTIONS GIVE YOU THE CAPABILITIES TO OPTIMIZE NETWORK PERFORMANCE

ixia
A Keysight Business

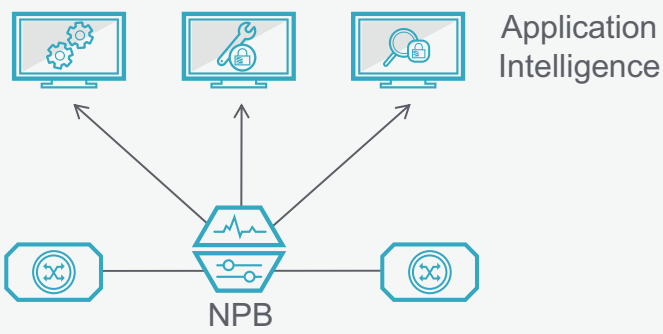
915-8138-01-9081 Rev B

50 - APPLICATION INTELLIGENCE IDENTIFIES SLOW OR UNDERPERFORMING APPLICATIONS

SOLUTION SUMMARY

- Use an NPB with an application level dashboard to observe applications in use and bandwidth consumption
- Identify bandwidth hogs and bandwidth explosions, e.g., Smartphone apps
- Use geolocation to show overloaded / underperforming network segments

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Application intelligence can be used to identify slow or underperforming applications. For instance, application information, flow data, and geographic information can be combined to show what applications are running on your network, how much bandwidth each application is using, and what the geographic usage is for the application. This solution allows you to isolate and filter traffic matching specific applications, geographies, keywords, and handset types. This data can then be exported to other applications, like a Splunk application or something, for long-term data collection and performance trending.

An NPB with application intelligence functionality allow you to access empirical data to identify bandwidth usage, trending, and growth needs. This empirical data can then be used to proactively manage network resources and new equipment installations, accurately forecast expansions, and perform better budgeting for expansions.

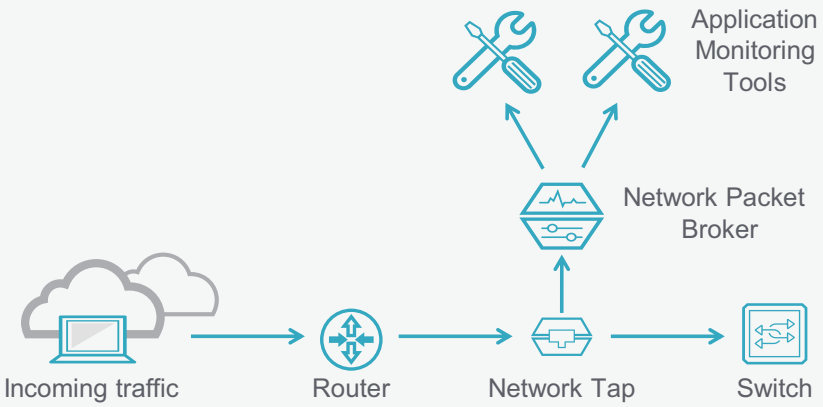
Once the data is collected, it can be exported as packet data or NetFlow information, depending upon the input required by your monitoring tools. The data can also be viewed natively in a dashboard for early access to the information and real-time analysis.

51 - APPLICATION PERFORMANCE MONITORING DELIVERS NETWORK OPTIMIZATION

SOLUTION SUMMARY

- 41% of IT personnel spend over 50% of their time working on network and application performance problems[55]
- Use an NPB with APM tools to quickly isolate and resolve application issues with better data monitoring
- Validate SLA performance for network applications

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

One of IT's main tasks is to ensure application availability across the network. This is a complicated task because of various parameters, including physical network effects, distributed employee network access, use of virtualization and cloud networks, assorted security threat controls, a multitude of device types in use, and network bandwidth limitations. Network administrators need application monitoring tools to help them discover, isolate, and solve problems related to applications. Various parameters require analysis, including client CPU utilization, data throughput, bandwidth consumed, application memory consumed, and geographic location of problems. Some tools even allow you to drill down into the application code to get even more insight.

APM solutions allow you to understand the performance of critical transactions happening on your network and correlate the transactions and data across your network. This information can be used to solve performance and availability issues. As an example, a common blind spot for hospitals is access to application data and application performance trending. In this case study, the customer was using the EpicCare Ambulatory Electronic Medical Record (EMR) application from Epic but was having problems correlating all of the information from their different systems. An NPB was deployed, which was able to aggregate data from the relevant sources, filter out the correct data, and then feed it to the customer's APM tool for analysis.[56]

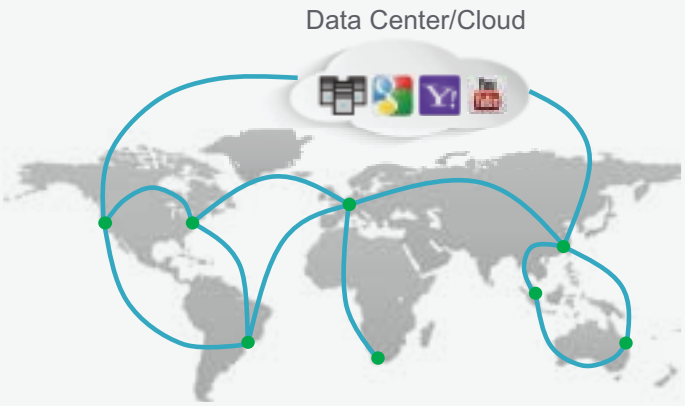
APM solutions can also be used to help with compliance of service-level agreements (SLAs). Business rules can be set to alert an administrator when there is a problem, ensuring that business-critical applications and functions are given priority. It is even possible to flag critical transactions and application performance to get information about error rates and response times. Some solutions also allow you to visualize performance metrics.

52 - PROACTIVE MONITORING CREATES BETTER AND FASTER NETWORK ROLLOUTS

SOLUTION SUMMARY

- 40% of network problems are detected and reported by end users[57]
- Proactively generate network traffic to test SLAs for on-premises and cloud networks
- Pretest how an application will perform on the network under load before your users do to create faster and better network upgrade rollouts

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Proactive monitoring uses visibility technology to actively test your network. According to the EMA Network Management Megatrends 2016 report, 40% of network problems are detected and reported by end users.[57] In addition, 26% report that one of their top networking challenges is the lack of end-to-end, multisite network visibility and troubleshooting capabilities. This is where proactive troubleshooting can help.

Proactive monitoring has several fundamental benefits including the ability to:

- Know immediately what the performance level of your network is
- Understand how well your applications are running
- Validate SLAs—both on-premises and in the cloud
- Test upgrades during maintenance windows before company employees do

Network performance and application performance may sound simple, but these can actually be difficult to ascertain. To get a true indication of network performance, the network needs to have a large amount of traffic on it, which makes you dependent upon peak busy hours. This solution allows you to place probes anywhere in your network and test whenever you want to. It also allows you to accurately simulate the right traffic so that APM tools can observe how well applications are truly performing. For instance, this allows you to simulate small packets or Skype-like data if you want to test your instant message (IM)/voice/video solution.

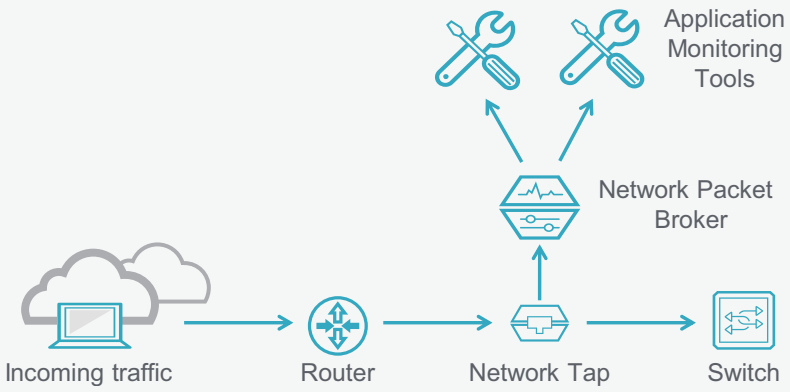
SLA validation can also be done during business hours, since it is not service disrupting. This allows you validate the SLA performance at will. The information gathered can then be used to inform management about which goals are being met. If goals are not being met, you can use the impartial data you have collected and contact your vendor to have them either fix any observed network problems, or give you a discount if they are failing to meet agreed upon SLAs.

53 - OPTIMIZE NETWORK PERFORMANCE MONITORING EFFECTIVENESS

SOLUTION SUMMARY

- Use an NPB to deliver all required traffic from anywhere in the network to the NPM tool to record 100% of the traffic for playback and analysis
- Support all network speeds (1G, 10G, 40G, 100G) or virtualized data ports with your existing NPM tool(s)
- Analyze the captured traffic for anomalies and quick problem resolution

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

NPM tools can be very effective at diagnosing network issues. NPM is comprised of software-based tools that can take metrics from your baseline analysis, flow data, and information that can come directly from your network devices to give you a complete picture of your network. However, standalone deployments of these tools can run into problems like: overloaded disk space and processing, the need for different interface ports based upon network traffic speed, and the needs for lots of input ports to capture data across the network. An NPB can be used to capture network data and filter that data before it goes to the NPM tool. This increases the efficiency of the tool by reducing clutter. The additional filtering of duplicate data further enhances the efficiency and also removes the storage waste associated with storing irrelevant data. Combining an NPM with a virtual tap and NPB also lets you use physical tools for the analysis of virtual data information to increase the efficiency of your NPM solution. In fact, an NPB can be used to deliver the following benefits:

- Aggregate data feeds from multiple sources (taps, SPAN ports, virtual taps, and data switches) and combine the information into a single data stream to the NPM tool
- Automatically filter out duplicate traffic to save tool disk space and processing resources
- Filter out uninteresting data to the NPM tool to make it more efficient
- Detect if the NPM tool is off-line and then immediately redirect traffic to another NPM tool on the network to provide redundancy/high availability
- Filters can be dynamically tightened as needed to ensure key traffic is always recorded
- Traffic can be load balanced across multiple NPM input ports to provide n+1 redundancy and also to spread higher data rate traffic across lower rate input ports on the NPM tool

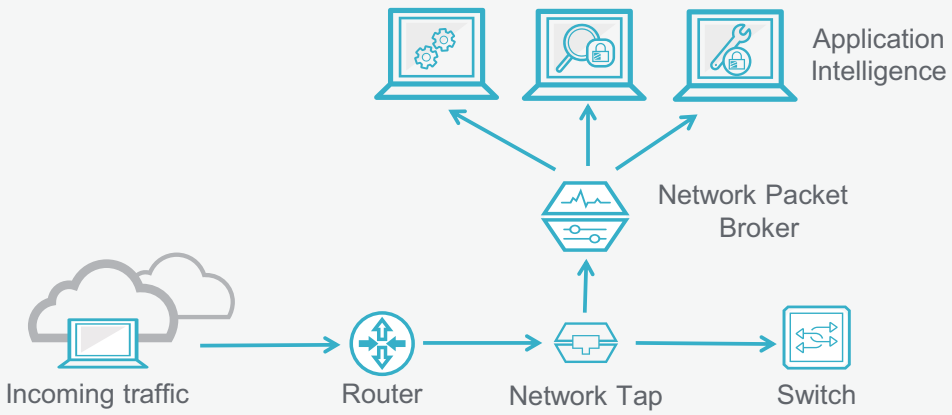
NPM tools and a visibility architecture can help you to stop missing critical network events. Instead, you can essentially rewind your network data to quickly troubleshoot sporadic performance problems. The NPM tools can also navigate to the exact moment a problem happened to show a detailed packet-level view of before, during, and after the occurrence.

54 - PREVENT APPLICATION BANDWIDTH OVERLOADS ON YOUR NETWORK

SOLUTION SUMMARY

- Data center network outages cost about $436,000 per hour[58]
- Use an NPB with application filtering to understand application and geographic uses of your network better
- Predict application explosions before they bring the network down

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Application intelligence information can be used to predict user and application performance. A fundamental benefit of this solution is that you can see if there are any bandwidth bursts or explosions happening. For instance, one mobile carrier a few years back had a situation where a new smartphone application was introduced. It was an interactive application between multiple users. Customers loved the app and usage skyrocketed. In fact, over the course of a couple weeks, the bandwidth consumed became exorbitant and the mobile carrier network actually crashed and was out of service for several hours—all because of this one application.

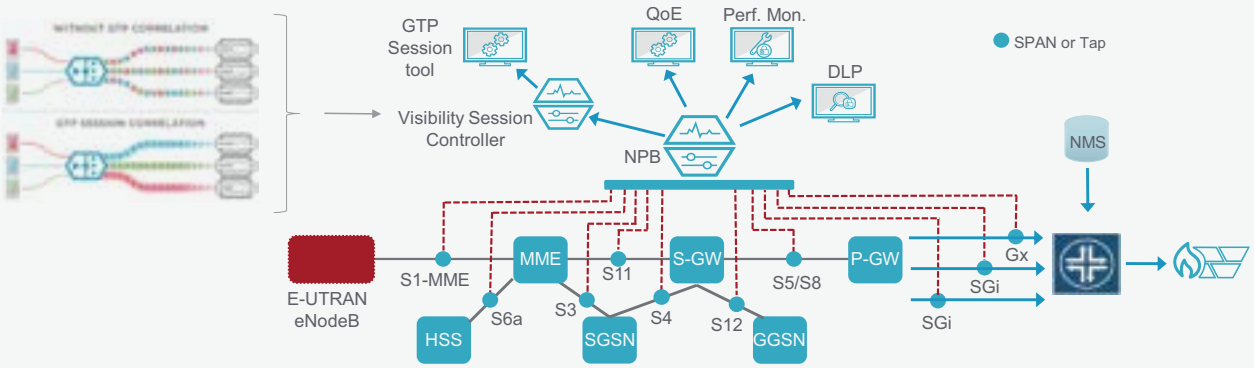
This resulted in a loss of revenue and a huge public embarrassment for the service provider—as the media picked up the story. Had the carrier been using application intelligence, the bandwidth consumption of that particular application would have shown up on the dashboard. The system admin could have easily seen the bandwidth explosion in real-time. Armed with that information, they could then have put controls in place which would have prevented the network outage.

55 - USE A GTP SESSION CONTROLLER TO IMPROVE CARRIER CUSTOMER QOE

SOLUTION SUMMARY

- Improve network service dependability and customer QoE
- Enable monitoring solutions to scale by offloading the correlation of subscriber data from monitoring probes to a GTP session Controller
- Sample and filter GTP sessions to reduce traffic sent to probes
- Automatically detect probe failure and redistribute traffic until the probe recovers

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Mobile carriers are continually looking to improve network service dependability and their customer's quality of experience (QoE) because this effort leads to higher levels of service assurance and increased revenue for mobile carriers. Service providers (especially wireless service providers) need good customer problem data (service holes, malfunctioning radios, poor coverage, and even customer dissatisfaction) to properly plan their networks and deliver a better quality of experience. An important element in this process is the use of sophisticated and costly network monitoring probes that allow mobile carriers to immediately detect and resolve issues that impact QoE.

While network probes can provide visibility into wireless core networks, these devices have limited capacity and may not withstand fluctuating mobile subscriber traffic. At the same time, the under-loading of network probes can create additional costs for the carrier.

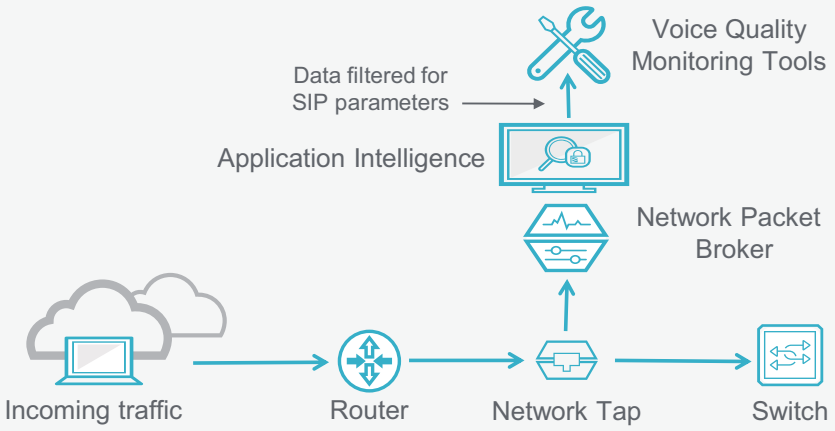
A GTP session controller can be used to effectively identify and track mobile subscribers. At the same time, it can correlate data from network probes which can be used to load balance bandwidth to enforce capacity and rate limits for each customer, even as mobile traffic rates fluctuate. If the controller detects faulty or overloaded monitoring probes, it automatically redistributes the load to other probes in the cluster. As a result, monitoring probes are able to focus on QoE analysis, rather than spend cycles trying to reassemble GTP session traffic. This allows you to maximize network probe capacity while improving visibility into the wireless core network.

56 - IMPROVE AND SIMPLIFY VOICE QUALITY MONITORING EFFORTS

SOLUTION SUMMARY

- 41% of IT personnel spend over 50% of their time working on network and application performance problems[59]
- Web conferencing companies can use an NPB with application intelligence to better segment monitoring data since they have separate tools for PSTN and native VoIP
- Application sub-definition information (e.g., SIP codec field) makes intelligent routing decisions for monitoring data possible

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

In addition to being able to detect application definitions running on a network, a proper application intelligence solution needs to capture and distinguish application sub-functionality as well. This application sub-functionality can be exploited to provide even more context-aware data processing capabilities.

For example, some SIP-based voice quality monitoring solutions need to understand whether the voice source was a traditional voice call or a digitally generated (voice over IP using a computer) call. They cannot just filter data based upon the SIP protocol because all of the connections are SIP at the monitoring point. Fortunately, the SIP protocol has a codec field that indicates the voice source. An NPB with application context-aware data processing capability can be used to read the codec field to understand the different source media types and pass that information along so that a copy of the traffic is routed to the right type of voice quality tool for proper analysis. The NPB can then send calls from different sources out different NPB ports to the appropriate monitoring tools.

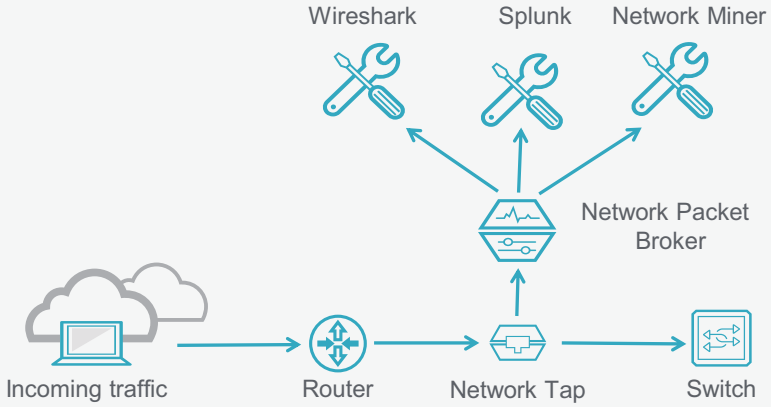
Information granularity like this reduces application troubleshooting costs and allows you to optimize customer quality of experience by providing the all-important details. It is one thing to know that something is happening, it is another to know why.

57 - FOCUSED DEEP PACKET INSPECTION OPTIMIZES YOUR NETWORK DATA

SOLUTION SUMMARY

- The global DPI Market is expected to reach 4.71 billion USD by 2020[60]
- Use of DPI can increase network performance and security
- NPBs with application intelligence can capture key information for data mining

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Deep packet inspection (DPI) is a general term for gathering extensive information from packet capture and analysis. According to Wikipedia, DPI is used to look at not only the packet header but the data part of a packet as well to gather information. Use of this data can improve network management, network security, and data mining. Examples include finding indicators of compromise, fault isolation, discovering performance impairments, exposing compliance/policy issues, and offering new services (like usage based billing or advice-based billing).

Additional benefits can be achieved using flow-based data to break down traffic metrics inside the network. You are able to go in and see (via a flow graph) exactly where all the traffic is being used. Depending on how you decide to configure this protocol, you can break down this information into IP protocols, UDP ports, and even user IDs or IP addresses.

There are essentially three levels of packet inspection:

- Deep packet capture
- Focused deep packet captures (events like security review)
- Deep packet inspection of the data portion of the data portion of the packet

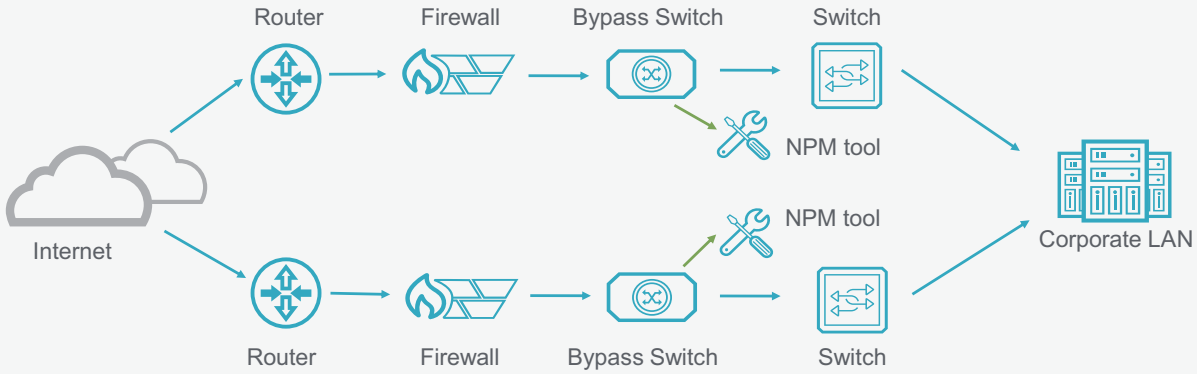
An NPB can then be used to filter the data as needed based upon specified criteria to look at almost any inspection parameter. This commonly includes Layer 2 through 4 information. Application intelligence functionality with the NPB can provide Layer 7 data as well. This data is then sent to various tools like Wireshark for packet capture analysis, NetworkMiner (which is network forensic analysis tool to help enforce policies and reconstruct events), The Dude (which is a network monitoring tool that monitors devices and alerts you when there is a problem), Splunk (which is a data collection and analysis platform of various items like event logs, devices, services, TCP/UDP traffic, etc.), and various other tools on the market.

58 - CONDUCT INLINE NETWORK PERFORMANCE MONITORING

SOLUTION SUMMARY

- 41% of IT personnel spend over 50% of their time working on network and application performance problems[61]
- Capture real-time network performance data to isolate real-time data delivery problems
- Use inline bypass switches and an NPB to deploy NPM tools to maximize network performance

Deployment scenario: Inline visibility architecture



SOLUTION OVERVIEW

Most use cases for inline visibility are security related but some are not. A couple cases include load balancing and NPM. By deploying the NPM solution inline, the IT engineer can get instant access to network activity, such as: bandwidth utilization, flow volume, application response times, and key network events.

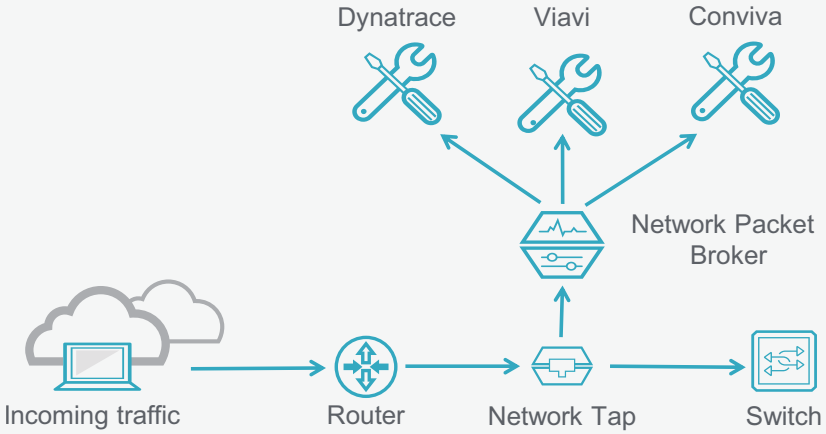
As an example, one use case for deploying an inline NPM solution involves understanding deployment differences for the corporate data backbone. This is a common use case for banking and financial trading organizations. For instance, if you have a dual core backbone that is deployed for redundant load sharing and notice performance differences between the two networks (e.g., data arrives faster on one network versus the other), the inline NPM solution will allow you to characterize both networks to isolate transmission speed differences. This is done by inserting a bypass switch into each network and then connecting both bypass switches to an NPM tool. The NPM can then analyze both networks in real-time to characterize the source of the problem(s).

59 - BETTER DATA COLLECTION MAKES QOE MONITORING MORE EFFECTIVE

SOLUTION SUMMARY

- Understanding how to use QoE can be a competitive differentiator
- 22% of enterprises surveyed are using NPBs to improve customer satisfaction[62]
- NPBs with application intelligence can capture key information for data analysis

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Quality of Experience (QoE) is a measure of the overall level of satisfaction with an application, connection, speeds, etc. QoE differs from Quality of Service (QoS), which embodies the notion that hardware and software characteristics can be measured, improved, and perhaps guaranteed, leading to network reliability and performance. QoE can be used to measure customer satisfaction, failed customer interactions, design flows (like user navigation across a website), and data that marketing can potentially use to optimize customer experiences on websites, portals, and such.

This data can be used by various businesses within industry segments, like healthcare, media, financial trading organizations, etc. to understand how customers are, and are not, using the business' website and services. Do problems exist? Do delays exist? If abandonment occurs, at what juncture and what was happening at the time. Organizations want to know ahead of time, not when a customer calls in to complain that a problem exists.

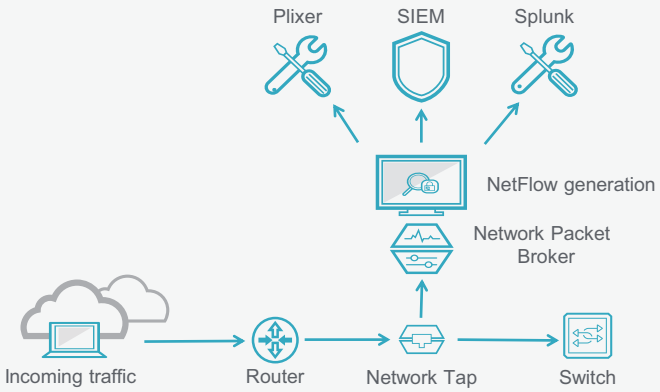
An NPB with application intelligence can be used to filter on certain criteria parameters like protocols (e.g., RTP report packets), application-level information (e.g., application type, application availability, application sub-functions used, etc.), and data from specific locations like VLANs. This data can then be fed to specialized tools for analysis. Just some of the examples include Dynatrace tools for application monitoring to diagnose Web user navigation experiences, player satisfaction monitoring using a tool from Conviva, and customer interaction experiences using tools from Viavi.

60 - OFFLOAD NETFLOW DATA GENERATION TO IMPROVE SWITCH PERFORMANCE

SOLUTION SUMMARY

- 49% of organizations surveyed are using network flow data for advanced analytics[63]
- NetFlow data provides summarized information on traffic applications and patterns for network optimization
- NPBs can generate NetFlow data and send to a NetFlow collector

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

NetFlow is a Cisco protocol that was developed 20 years ago to help IT engineers gain insight into their network. Detailed packet captures are often the best source of insight (because it contains the payload information) but increasing network speeds and the effort needed for packet captures is making flow data even more useful. Instead of capturing origination, destination, ports, protocols, etc. for one data stream, NetFlow (and the IETF version called IP Flow Information Export (IPFIX)) aggregates this information for multiple data streams to illustrate what is happening across the network. This information can be used to: see resource utilization across the network, improve troubleshooting, capture signs of unauthorized traffic, see data exfiltration, validate QoS parameters, expose denial-of-service attacks, and much more.

However, there are some issues associated with NetFlow:

- Older Cisco switches cannot generate this data
- Newer Cisco switches can become loaded down if this feature turned on
- Cisco is the only network switch vendor that generates this data

The solution is to add an NPB to your network. An NPB can be used to generate NetFlow data and send that data to a NetFlow collector, such as a SIEM, Plixer device, or Splunk device. For instance, one of the main issues with NetFlow/IPFIX is that it can overburden the routing switch during high utilization. As the CPU for the routing switch reaches maximum capability, it will start to shed load, which means that NetFlow data can be impacted, i.e., slow response times or gaps in data capture. An NPB that supports NetFlow can be used to offload this functionality from the routing switches. When combined with context-aware data processing, the NPB can deliver application intelligence far beyond what the Cisco switch delivered natively.

Strengthen Regulatory Compliance Initiatives

REDUCE COSTS, MINIMIZE SECURITY RISKS, AND ELIMINATE POTENTIAL COMPLIANCE FINES

ixia
A Keysight Business

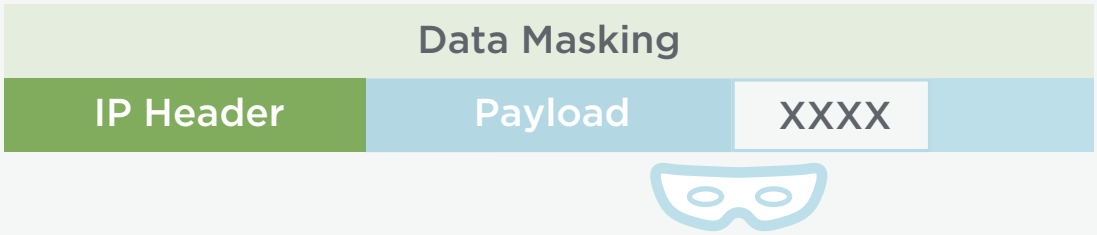
915-8138-01-9081 Rev B

61 - ENHANCE REGULATORY COMPLIANCE WITH DATA MASKING

SOLUTION SUMMARY

- Enhance regulatory compliance by using data masking of sensitive information
- Data masking is one of the Top 5 most commonly used NPB features[64]
- NPBs can mask data and forward it to specific analysis tools for inspection

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Regulatory compliance is a known concern for enterprises. Just when you think you have got the network correctly set up, some company business decision adds or removes new products and applications to the network, which can cause new compliance issues for you. For instance, regulations over the last several years typically demand that personally identifiable data be secured whether at rest, in motion, or in use.

A common way to secure this data in monitoring solutions is to add masking of the data to protect it as it is passed downstream to other tools. Packet data can be analyzed in real-time and replaced with a fixed-field value before forwarding to security and monitoring tools. This is one of the top five most commonly used packet broker features, according to a research survey conducted by EMA in 2016.[64]

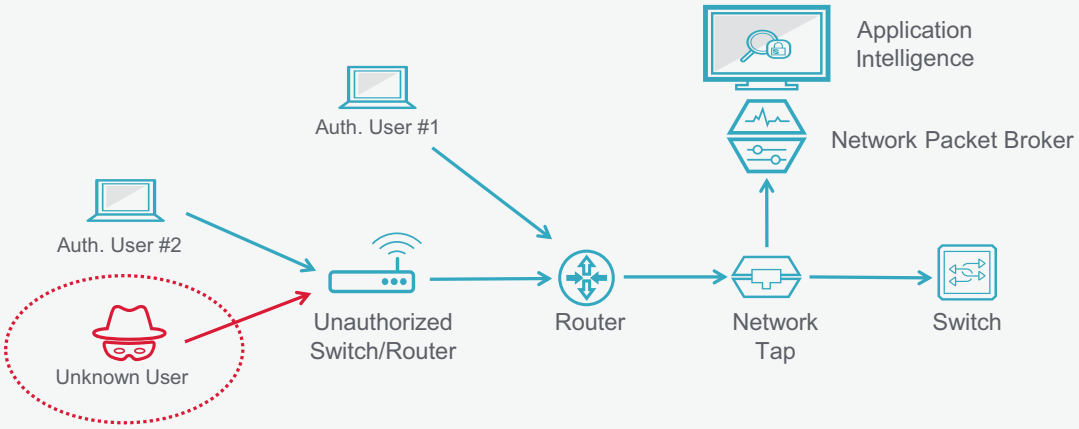
Once the data is masked, it can still be used. For instance, for credit card data you would only mask the first 12 digits and leave the last 4 unmasked. This would allow tools to search the data to find specific credit card number usage. Maybe you leave the first digit unmasked, as well. This allows your tools to perform searches to categorize the types of credit cards in use—American Express, Visa, Master Card, Discover, etc. The level of masking is user determinable.

62 - DISCOVER ROGUE IT ON YOUR NETWORK

SOLUTION SUMMARY

- Deploy an NPB with application intelligence to discover unauthorized activity
- Identify user equipment and device types that are added to the network
- Detect application signatures of applications not authorized for the network
- Protect against unauthorized use of network resources

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Rogue IT is when users add their own equipment and applications to the network. This includes items like portable Ethernet switches, Wi-Fi access points (like a Wi-Fi hot spot from an iPhone), use of off-network data storage (like Dropbox), or when anything else is added to the network. All of these examples should (as a best practice) be violations of company security policies, because they introduce the potential for unknown security attack vectors. IT rarely knows anything about these devices, especially as they can appear sporadically, like Wi-Fi hot spots.

To thwart these compliance and liability threats, you need the ability to detect application signatures and monitor your network so that you know what is, and what is not, happening on your network. This allows you to see rogue applications running on your network along with visible footprints that hackers leave as they travel through your systems and networks. Application intelligence can expose hidden applications, geolocation of users, browser types in use, and device types on the network.

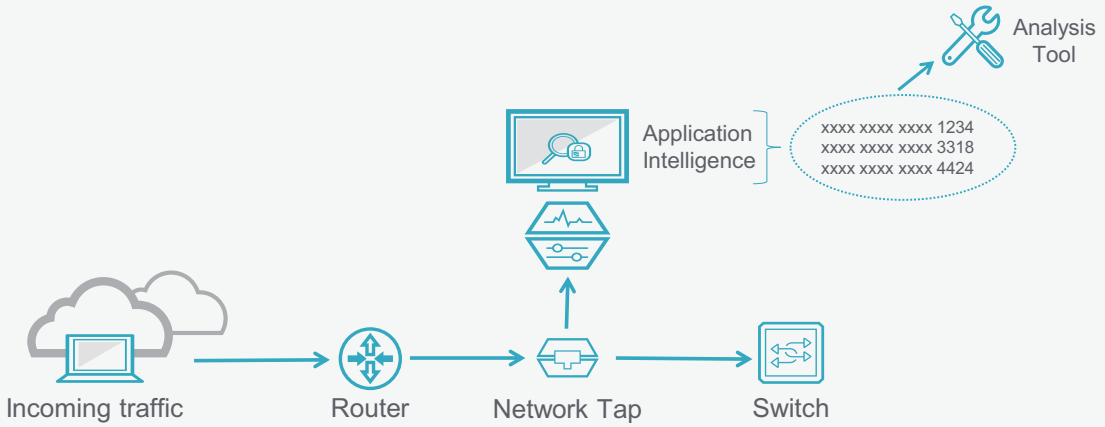
As an example, there have been instances where an employee has created an insecure hot spot within a corporate office that a hacker can use for criminal activity. The hacker could sit outside the office in a van on a public street and use the hot spot to gain access to the Internet through the corporate routers. Once on the Internet, the hacker can conduct all sorts of cybercrime (illegal trading, identity theft, cyber espionage, communication with terrorist organizations, child pornography, and the latest craze of Hacktivism for political, social, and religious reasons) that would all be traced back to that particular business (and that particular hot spot) by law enforcement agencies. This could legally incriminate the company and the employee who installed the hot spot. In the end, this behavior could cost both the business and the employee (possibly soon to be ex-employee) lots of time, energy, money, and aggravation to clear their name(s).

63 - SEARCH FOR AND CAPTURE SPECIFIC DATA WITH APPLICATION INTELLIGENCE

SOLUTION SUMMARY

- Use an NPB with application intelligence to perform granular Regex data searches
- Forward specific data to monitoring tools for further analysis
- Lower your CAPEX for security and monitoring tools

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Regular Expression (Regex) searching is another application intelligence capability that can be enabled to let you search the monitoring data. Once the specific information, or type of information, is found that matches the search criteria, that data can be sent to a security analysis tool (e.g. DLP or something) for processing. This search capability allows your tools to be more effective as they have less data to sift through.

Specifically, Regex allows you to perform vary granular searches for data like credit card numbers, phone numbers, social security numbers, emails from certain IP addresses, names, phrases, or specific numbers. By using an NPB with application intelligence to perform the data searches, CPU resources on more expensive monitoring tools can be freed up. This increases the efficiency of the monitoring tools and potentially lowers your CAPEX costs as you may be able to purchase fewer tools but still accomplish your goals.

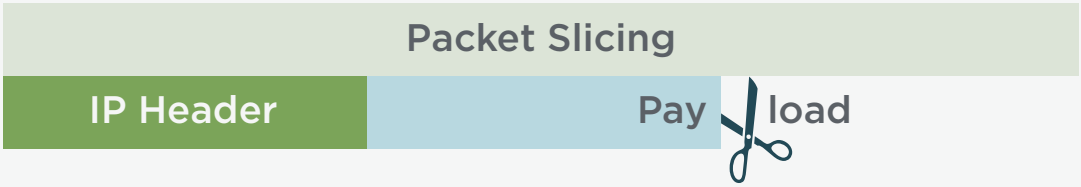
As an example, an NPB with application intelligence could be used to capture credit card data and then send that data to a purpose built tool to analyze the number using the Luhn checksum algorithm. All valid credit card numbers adhere to the Luhn algorithm, which is a special formula that sums all the digits to come up with a multiple of 10, if the number is valid. If a credit card number fails the test, it can immediately be flagged as fraud. A faster fraud determination can lessen the chances of monetary losses due to fraud. Luhn checksum analysis can be used for other systems, like Canadian and Greek social security numbers, besides credit card numbers.

64 - PACKET TRIMMING ELIMINATES SENSITIVE DATA PROPAGATION

SOLUTION SUMMARY

- Use an NPB to remove sensitive data, like credit card data, phone numbers, social security information, etc.
- Data removal reduces the load on the tools by reducing packet size, which frees up long-term storage of unneeded payload information
- Packet slicing can reduce monitoring data traffic bandwidth up to 70 to 80%[65]

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Packet trimming (payload stripping) removes the payload data from the packet, leaving only essential envelope information, prior to sending the packet to monitoring tools. The amount of packet trimming is user definable, e.g., all of the payload, part of the payload, etc.

This feature allows the tool to be more efficient and analyze incoming data faster. Some monitoring tools do not require packet payload information, in which case removing payload data allows more data to be sent across the link from the network monitoring switch to the monitoring tool. As a result, the monitoring tool can process a greater amount of network data.

A second example for packet slicing is that once the payload is removed, the sensitive personally identifiable information is gone, as well. The personal data is protected and the monitoring data can be passed downstream to monitoring tools without the worry of a regulatory compliance infraction.

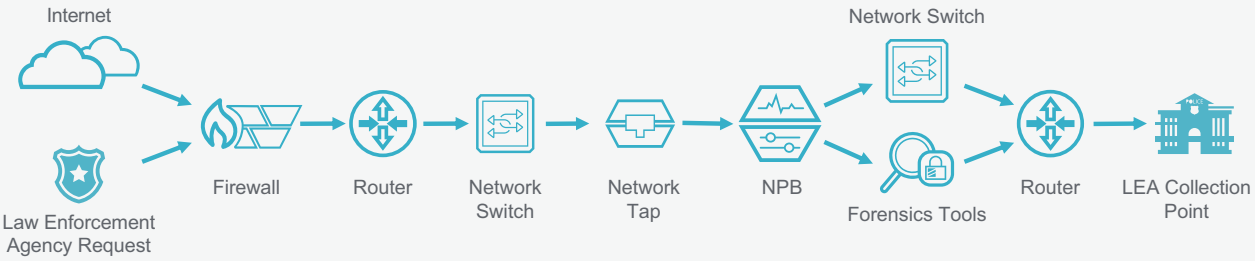
There is a trade-off though. Unlike data masking, the payload data cannot be searched once removed, as it is gone forever. So if that is a concern, you should take the data masking approach. Otherwise, you can use this approach.

65 - PERFORM LAWFUL INTERCEPT DATA CAPTURES

SOLUTION SUMMARY

- Lawful intercept requests for carriers and ISPs continue to increase annually[66]
- An NPB can be used to filter the information sought in a warrant
- Only relevant pieces of data are sent to the law enforcement agency

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

The ability to support lawful data intercept is becoming increasingly important for service providers. At the same time, this has become a new challenge for enterprises. For instance, some search engine Internet companies are seeing an increase of almost 20% per year in the number of lawful intercept requests they receive.[66] Legally mandated access to communications is expanding as many of the world's nations write laws requiring access to all types of user information, including voice, video, data, and even location information. It does not stop there, because the requirements and legal application of laws vary by country as well as by different states.

Some think that the Communications Assistance for Law Enforcement Act (CALEA) only applies to the PSTN or wireless carriers, they would be wrong. Lawful intercept orders are being issued to ISPs as well. Entities that have user communication content can overlap in the Big Data era. This includes voice communication, video, instant messaging, facsimile, Internet connections, digital pictures, text messages, data downloads, file transfers, etc. One or more of these content streams could be requested under a lawful intercept order. Depending upon the number of user communication services that an entity provides, it can get very complicated to comply with lawful intercept requests.

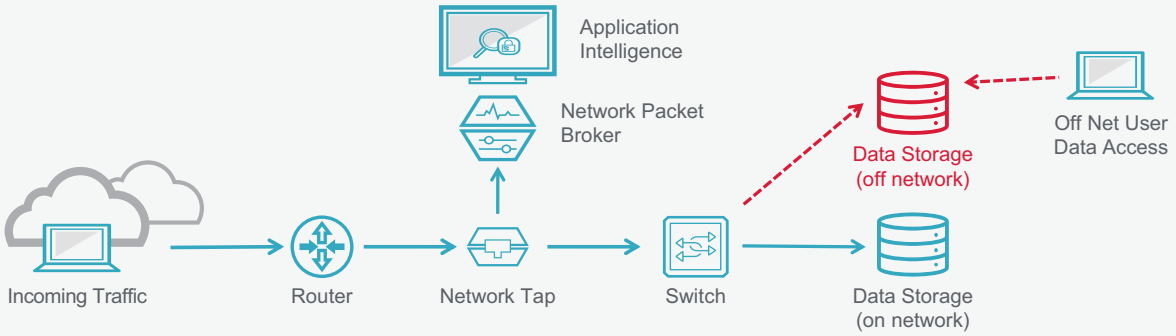
The next question is how to capture the information. You will want to use a filtering device to capture and filter the data to get the required information so that you can aggregate and segment the necessary data. An NPB contains the ability to deduplicate unnecessary data, create detailed filtering rules to segment data packets, provide the necessary aggregation of the appropriate lawful intercept data required, and then finally send it downstream to the appropriate collection point for the Law Enforcement Agency (LEA). NPBs can process data at line rates and eliminate concerns of tainted evidence. The filtering device should be a firmware-based device, not just a SPAN device. Without a filtering device, lawful intercept will become an expensive and painful activity for you as you try to separate the relevant and non-relevant packet data with other devices.

66 - ENFORCE IT NETWORK SECURITY AND COMPLIANCE POLICIES

SOLUTION SUMMARY

- Use an NPB with application intelligence to validate IT policies
- Monitor cloud application usage of non-sanctioned storage apps, like Dropbox
- Understand if non-company standard email services (like Web-based mail services) are being accessed and files downloaded through Web-based email bypassing virus inspection
- Reduce company risk with a defined policy and method to enforce it

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

A fundamental concern for IT is to enforce security and regulatory compliance of network policies. In several cases, they may honestly not know what is happening on the network. This issue has been top of mind for enterprises for several years—how can they reduce corporate risk? Part of the solution is policy-related, but they also need a way to show due diligence to enforce the policy.

One example is to use context-aware data processing to monitor cloud application usage. For instance, application monitoring lets you know that employees may be using services like Dropbox to transfer company files and bypass your security policies. Once an employee is no longer employed by the company, they could still have access to those files, since IT cannot restrict the privileges to off-network storage devices.

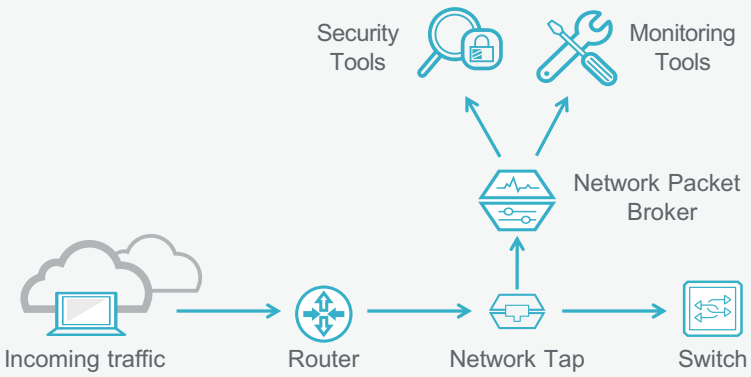
Another example is where employees may be using other, non-company standard email services (like Web-based mail services) to access and download files. This use case usually involves accessing media that does not go through anti-virus/malware inspection and can, therefore, pose a security threat to the corporate network, especially regarding file downloads. These practices could introduce ransomware or open up security holes in the network for hackers. Application intelligence provides a way to expose if there are specific policy violations happening on the network.

67 - DOCUMENT SECURITY POLICIES FOR REGULATORY COMPLIANCE

SOLUTION SUMMARY

- 72% of companies surveyed plan to enhance the quality, availability, and timeliness of risk data[67]
- Create empirical data to validate that network policies and procedures are working correctly
- Properly document data at rest, in use, and in motion for regulatory compliance

Deployment scenario: Out-of-band visibility architecture



SOLUTION OVERVIEW

Regulatory compliance requires that companies secure their network data at rest, in use, and in motion. This requires documenting the plans and procedures in writing. It also involves capturing the data needed. According to a Deloitte University survey, 72% of companies surveyed plan to enhance the quality, availability, and timeliness of risk data.[67] However, you also need to document the validation of these policies. Validation is fairly straightforward and can be accomplished with a visibility architecture.

It starts with capturing the data for both inline and out-of-band data monitoring architectures by using taps, virtual taps, and bypass switches. Once the data is captured, it should be run through an NPB. The packet broker provides data filtering to send the right type of data to the right type of security tools (firewall, NGFW, IPS, IDS, DLP, SIEM, etc.) and the right type of monitoring tools (NPM, APM, proactive monitoring, analyzers, log analysis, packet captures, etc.). The NPB can provide granular filtering to ensure that tools in use are actually working correctly. An NPB can also be used to apply application intelligence to metadata to illuminate even more information about network policies and procedures.

The visibility architecture allows you to verify who and what are on your network, create a dependencies profile, create an IP address to MAC table, apply application intelligence to monitoring data, capture and deliver granular data, and validate (with empirical data) that the network policies and procedures put in place to protect network data are working correctly.

CONCLUSION

Network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. There are many use cases that can be deployed to solve or enhance issues that IT monitoring and security engineers face. The key point is to implement a visibility architecture that creates the fundamental capture and sharing of the valuable data that is needed.

Use cases based upon a visibility architecture will allow you to do the following:

- Access the data you need, when you need it, across the network to properly diagnose problems
- Add/remove security, forensic, and monitoring tools at will for inline and out-of-band monitoring architectures
- Decrease mean time to repair
- Provide a rapid response to crises
- Conduct advanced threat analysis
- Eliminate most, if not all, Change Board approval processes and crash carts for monitoring efforts
- Reduce the cost of a breach by connecting tools to the network faster and decreasing the associated MTTR
- Reduce your tool (and SPAN) port programming effort and costs
- Create an architecture that allows you to deploy new inline and out-of-band monitoring solutions

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

ENDNOTES

1 https://www.ixiacom.com/company/blog/blind-spots-abcs-network-visibility

2 https://www.ixiacom.com/solutions/visibility-architecture

3 2017 Trustwave Global Security Report

4 Ixia conducted research with customers

5 Enterprise Management Associates conducted research, October 2016

6 2016 Verizon Data Breach Investigation Report

7 2016 Trustwave Global Security Report

8 Cisco Systems – The Zettabyte Era: Trends and Analysis

9 Ixia case Study – University of Texas Secures Network While Controlling Costs

10 Ponemon Institute – Cost of Data Center Outages, January 2016

11 Enterprise Management Associates conducted research, October 2016

12 Blue Coat Infographic: Stop Attacks Hiding Under the Cover of SSL Encryption

13 Roi Perez. "Zscaler reveals risk of SSL based threats, warns of new security priority," SC Magazine. March 16, 2017

14 Ponemon Institute – The Cost of Malware Containment 2015

15 Cisco Systems – The Zettabyte Era: Trends and Analysis

16 Technavio – Global Deception Technology Market 2016-2020

17 Ixia conducted research with customers

18 Ixia conducted research with customers

19 ZK Research survey – Tempered Networks simplifies network security

20 Ixia conducted research with customers

21 Enterprise Management Associates conducted research, October 2016

22 Enterprise Management Associates – Network Management Megatrends 2016

23 Ixia Case Study – Company Reduces MTTR By 75% And Strengthens PCI Compliance

24 Ixia conducted research with customers

25 Enterprise Management Associates conducted research, October 2016

26 Dimension Data – Network Barometer Report 2015

27 The Telegraph – High-frequency trading: when milliseconds mean millions

28 Ixia Case Study – A Logistics Firm Saves Money and Speeds up Mean Time to Repair 80%

29 Ponemon Institute – Cost of Data Center Outages, January 2016

30 ZK Research – Simplified Programming of a Visibility Layer Can Have a Big Impact on Application Performance

31 Ponemon Institute – Cost of Data Center Outages, January 2016

32 Enterprise Management Associates – Network Management Megatrends 2016

33 Zeus Kerravala, ZK Research

34 Ponemon Institute – Cost of Data Center Outages, January 2016

35 Follow-up Material is available on baseline monitoring

36 Ixia conducted research with customers

37 ZK Research – Simplified Programming of a Visibility Layer Can Have a Big Impact on Application Performance

38 Ixia conducted research with customers

39 Veeam Data Center Availability Report 2014 – The Challenge of the Always-On Business

40 ZK Research – Simplified Programming of a Visibility Layer Can Have a Big Impact on Application Performance

41 2016 Verizon Data Breach Investigation Report

42 Ponemon Institute – 2015 Cost of Cyber Crime Study

43 Enterprise Management Associates conducted research, October 2016

44 Ixia customer research survey 2015

45 Cisco Systems – Cisco Global Cloud Index: Forecast and Methodology, 2015–2020, 2016

46 Enterprise Management Associates – Network Management Megatrends 2016

47 RightScale 2016 State of the Cloud Report

48 Ixia Case Study – Company Reduces MTTR By 75% And Strengthens PCI Compliance

49 Forbes blog by Eric Savitz. Gartner: 10 Critical Tech Trends For The Next Five Years, 2012

50 Cisco Visual Networking Index: Forecast and Methodology, 2015–2020

51 Taps vs. SPAN Full Visibility into Today's Networks

52 M&A Institute – M&A Statistics

53 McKinsey & Company and University of Oxford – Delivering large-scale IT projects on time, on budget, and on value

54 TechTarget – What is a sandbox?

55 Enterprise Management Associates conducted research, October 2016

56 Ixia Case study – Children's Health Care System Improves Visibility and Solves Application Performance Issues

57 Enterprise Management Associates – Network Management Megatrends 2016

58 Ponemon Institute – Cost of Data Center Outages, January 2016

59 Enterprise Management Associates conducted research, October 2016

60 DPI Market Share Analysis, Deep Packet Inspection Industry Report, 2020. Grand View Research, June 2014

61 Enterprise Management Associates conducted research, October 2016

62 Enterprise Management Associates conducted research, October 2016

63 Enterprise Management Associates – Network Management Megatrends 2016

64 Enterprise Management Associates conducted research, October 2016

65 Ixia conducted research with customers

66 Best Practices for Lawful Intercept in Service Provider and Enterprise Networks

67 Deloitte University Press – Global Risk Management Survey, 10th edition

ixia

A Keysight Business