Optimizing Network Design
In Security Projects

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Network security is top of mind in every organization. These days companies try to protect key customer data and intellectual property from cyber-criminal threats that have become increasingly sophisticated. As IT looks to strengthen their borders and proactively guard against suspicious behaviors, security specialists are sourcing and deploying a range of solutions including next-gen firewalls, intrusion prevention systems, data leakage prevention systems, web content filters and forensic analyzers.

At the beginning of each project, security specialists carefully scrutinize vendor specifications to ensure that each element in their security solution stack will provide the added protection they need.

However, many neglect a critical piece of the puzzle – network connectivity. Whether you are deploying a next-gen firewall or a forensic analyzer, preparing an accurate network design schema to support the solution is the first step towards optimizing results.

After all, security products can only do their job properly if they see every bit, byte and packet® that travels in and out of the network.

Best Practice Network Connectivity Models for Security Solutions

As with any IT project, there is a best practice method and then there are attempts to just make it work. Security connectivity is no exception. How an individual security appliance connects to the network directly impacts the type of traffic data they receive, and therefore, how well they can protect company assets.

Often, companies try to take advantage of existing "breaks" in the network (between the switch and the router) or try to tap feeds originating from the network elements (a switch's SPAN port or exports from network management tools) to send traffic to their security appliances. Unfortunately, these approaches have inherent design flaws.

Any security device plugged directly into the network can (and will) actively change the traffic that flows through it – especially when traffic levels spike unexpectedly. These distortions can manifest themselves as timing issues (frames no longer align), performance delays, dropped packets or simply an inability to process all the data that comes through the appliance. With no way to capture, store and correlate traffic – without impacting it – the direct connect method cannot be considered best practice. Obviously, collecting traffic from other live network elements has all these problems and more.

Only a truly "neutral" access method such as a network TAP can be considered best practice from a network design perspective. As a purpose-built hardware-only solution, a network TAP provides a

passive splitting mechanism whose only function is to copy network traffic and send it to secondary devices for analysis and/or storage. In the end, a "connectivity platform" enabled by network TAPs offers a best-practice methodology for providing every element in the security solution stack – from next gen firewalls to forensic analyzers – with 100% visibility into traffic flows from any point inside or outside of the network.

As you can see, this methodology supports a wide range of security projects including:

Optimizing Firewall and In-line Application Deployments

Firewalls, intrusion detection, content filtering, data leakage prevention, application layer protocols and other solutions that analyze traffic in real-time are a company's first and most important line of defense. Their job is to sniff out suspicious behaviors and shut down any transaction that violates defined security policies. With a network TAP in place, security specialists gain a failsafe access to network data – even when the power goes out.

For an additional layer of security, it is important to place a network TAP outside of the network as well in order to spot malicious activity in traffic outflows. Cyber criminals often attack firewalls and other in-line devices and alter them to make it appear as if everything in the network is functioning properly. Once that work is done, they will move on to more damaging activities and start hacking into key customer and corporate data stores. Only by examining outgoing traffic streams can a company determine if malware or phishing software has been injected into the network.

Firewalls and in-band solutions of any kind that alter traffic flows can wreak havoc on the other applications around them. Security specialists whose appliances are connected via a network bypass TAP can better mitigate potential problems arising from mis-timings and other conflicts. Because they let administrators easily move appliances from an in-line status to out-of-band, they help companies

quickly troubleshoot any issue that may arise. More importantly, the ability to take firewalls offline – without preventing them from receiving traffic data – means that administrators can easily upgrade systems and implement new policy controls without compromising security or network performance.

At the same time, bypass TAPs monitor the health of the devices as they communicate with them and will even route traffic to different appliances in the hierarchy in the event that one fails or becomes compromised.

Mitigating DoS and DDoS Attacks

Denial of Service (DoS) or Distributed Denial of Service (DDoS) are two of the most frequent and disruptive of attacks an organization can face. DoS attacks are a tactic hackers use to temporarily or permanently interrupt the connection between a host and network. DDoS attacks are more extreme and involve a large number of hackers simultaneously trying to shut down a target from multiple angles. Once the website is shut down it must restart itself which can take a significant amount of time depending on how overwhelmed the site was. During the restart, hackers typically try to inject malware in the site and infect it.

A network TAP is critical for mitigating risk when these types of attacks occur. Inserted on the outside of the firewall, it can collect important details on the attack itself which can be used to counteract its effect in the future. More importantly, it will collect data on the traffic flowing out of the network which will allow companies to quickly see if malware has compromised the company in any way (i.e. too much traffic flowing from the webserver to a specific IP address, etc.).

Enhanced Computer Forensics & Data Capture Techniques

Forensic data capture, pattern analyzers and other out-of-band offer solutions collect traffic data to reconstruct crime scenes and comply with legal and regulatory requests in the event that a breach does occur. It lets companies see which systems have been compromised and determine if customer information or IP has been actually been stolen in the process. Without proof, they may be required to contact customers in the event a security issue of any kind does occur.

Forensic solutions need a network TAP to ensure that they see 100% of the traffic – if there are gaps in the traffic flow, they may not be able to piece together what happened. However, companies that deploy network TAPs in different place can compare data to see where and how traffic changes between different network elements – an advantage that will significantly shorten time to discovery and hopefully help specialists shut down the connection before sensitive information is compromised.

It is also important to note that a network TAP remains functional even when the network goes down or loses power. This ensures that companies retain all the information they need to investigate breaches, even when hackers tamper with systems internally.

Enabling Lawful Interception

Managing regulatory requests for specific documents, emails, phone records and other "private" communications is a top priority for many security teams. Today, every country enforces lawful interception differently and national laws can vary from industry to industry. However, all companies must be able to address data capture warrants and give law enforcement access to conduct authorized surveillance activities quickly and efficiently without exposing the company to further risk.

When companies do need to provide official access to their public or private network's communication, those that use a network TAP fare better than those that do not. A network TAP guarantees that any lawful intercept solution in place has 100% of the data the agency is seeking. Those that do not may be forced to manually dig through log files and system records to produce the required information.

Design & Implementation Notes

Clearly, the way in which each element in a security program connects to the network is critical to its performance. Consider the following when designing a network connectivity plan for your next security project:

Know the Network Requirements

From the start, it is important to match the network TAPs specifications to your environment's exact requirements. That means investigating the types of cabling used (copper or fiber options) as well as the speed at which it currently operates (1G, 10G, 40G, 100G). Armed with this data, you can determine which network TAP is best suits your specific needs.

Determine the Access Points

Prior to installing any security solution, it is important to decide what kind of data you want to collect and how many points throughout your network do you want to tap. Being able to compare traffic flows from inside the firewall to the traffic outside can help identify harmful activity and cases where critical data is being steadily sent to a specific IP address. Similarly, analyzing data before and after it flows through the web application servers can reveal suspicious behaviors that need to be investigated.

Identify your traffic collection points beforehand to optimize the network design and connectivity plan from the start.

Load Balancing

Load balancing is a critical part of any security strategy – if firewalls and other solutions can't handle traffic spikes and packets are lost to any of the connected appliances, they may as well be turned off. By combining a hybrid packet broker and a bypass TAP, you gain both load balance and filtering along with traditional network TAP technology. This mitigates risk by allowing session aware traffic flows to be stored and analyzed as soon as resources become available. Without this step, you will need a sophisticated policy control algorithm in place to be sure security devices are not overridden in favor of business critical applications when network resources are scarce.

Providing a strong foundation on which to build a comprehensive security program is critical in an era when cybercrime threatens almost every company in business today. A best-practice connectivity design featuring network TAPs will provide critical visibility and flexibility as you move throughout the security solution lifecycle (deploy, update, augment, etc.). By eliminating any gaps in how appliances analyze traffic, you are effectively sealing up many of the avenues that hackers typically exploit when they attack a company's defensive systems.

In the end, network design is critical to any security strategy and should be evaluated with as much care as any other element in the solution stack.

For additional design tips, visit Garland Technology

To learn more about creating a comprehensive network design, contact the experts at Garland Technology.

GARLAND TECHNOLOGY

See every bit, byte, and packet®

www.garlandtechnology.com