Gawain Research

# How can firewalls keep up the pace in the "New Internet Era"

## -Hillstone T-Series intelligent Next-Generation Firewall Testing Report-


This is not the first time that Gawain has tested the Hillstone solutions, but it's the first time we have tested the Hillstone intelligent Next-Generation Firewall (T5060). From the UTM to NGFW to iNGFW, Hillstone maintains innovation and product upgrades at its own pace. But in the new internet era, with serious competition in the network security industry, what differentiators can we find with the Hillstone iNGFW after this test?

### Granular Traffic Control

The landscape for enterprise IT has changed in the new era; internet access has become more and more sophisticated. For many enterprises, a fast and robust network has become a basic working condition. The manner in which employees use the network and their satisfaction levels have also changed dramatically. For example, development teams mandate fast downloads of new system images. The marketing team demands a certain quality level for online media streaming and services. Account managers in the field demand access to marketing and sales

collateral for their clients over a shared network resource. Certain businesses that were not regarded as critical in the past have now become potentially powerful tools for improving productivity.

As a gateway at the edge of the network, next-generation firewalls have to accommodate these changes in the network landscape as well as link consumption.

When Hillstone launched its iNGFW, we had discovered a new feature – URL-based routing – and enabled it on the testing device. This feature is very valuable since traditional industries and enterprises can schedule traffic more accurately, optimize link efficiency and reduce the cost.

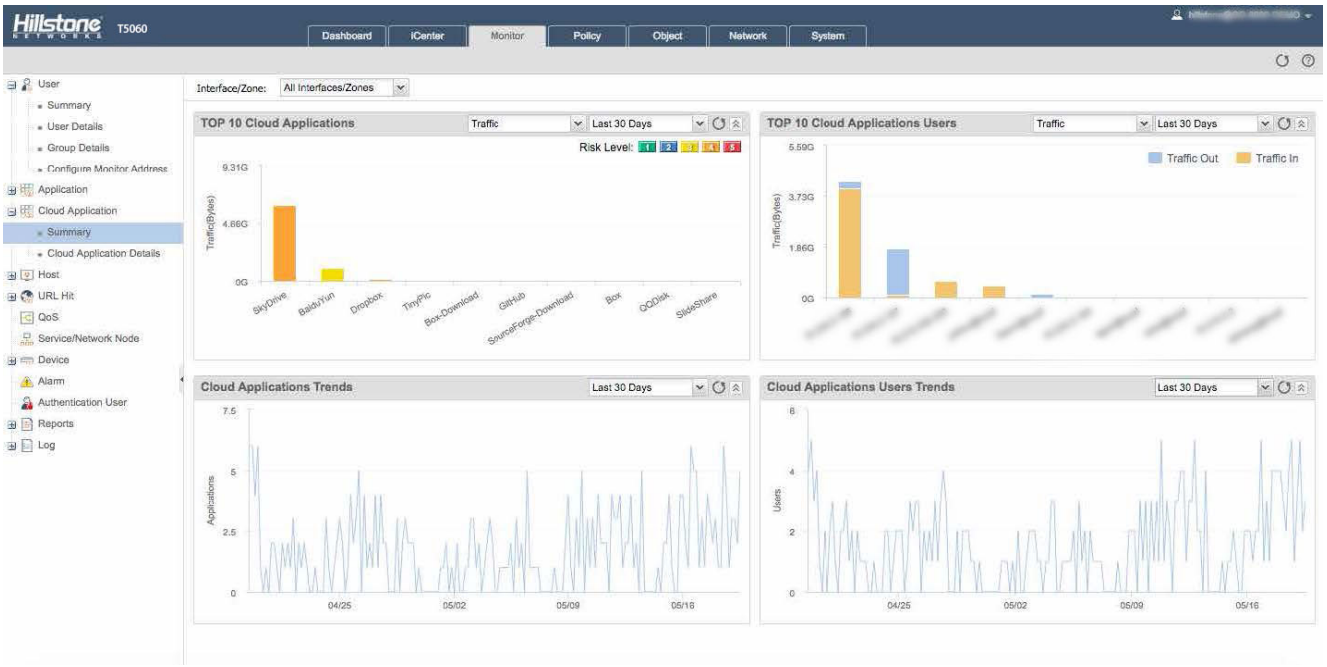
For example, the R&D departments for almost all the companies typically access github.com in order to accomplish their work. In addition, cross-functional product peers typically access developer.apple.com. As these are not local sites, it is necessary to perform data interaction with servers in Hong Kong (China), Japan, Taiwan (China), Singapore and some other countries. Given the increasingly congested international ports, we frequently found cases where connectivity to outside networks were either too slow or not functioning at all. Obviously, this had a large impact on overall productivity .

To address network latency, some enterprises purchased faster access links. As such links are extremely expensive, it is impossible as well as unneccesary to have all users access those links. However, for most devices, granting access to specific users cannot be solved even if routing is based on destination IP or applications. But we found that the T5060 adds URL-based routing that supports routing based on domain whitelist, providing the most critical offloading model for customers.

## Cloud as a Service

Today, media streaming and cloud storage are considered as key business applications. Therefore, we should guarantee their stability and effectiveness. Undoubtedly, it is ideal to route bandwidth-consuming applications that are not business critical to secondary or tertiary carrier links.

Same as other Next-Generation firewalls, the T5060 supports application-based routing, which is also one of the highlights in Hillstone’ s next-generation firewall offerings. Unlike most competitors, however, the T5060 separates “Cloud application” at the application-layer, which is a distinct characteristic and competitive advantage. In essence, this special dimension covers all the mainstream commercial B/S platforms and application. The T5060 supports independent operations of routing, traffic control, reporting and security protection.

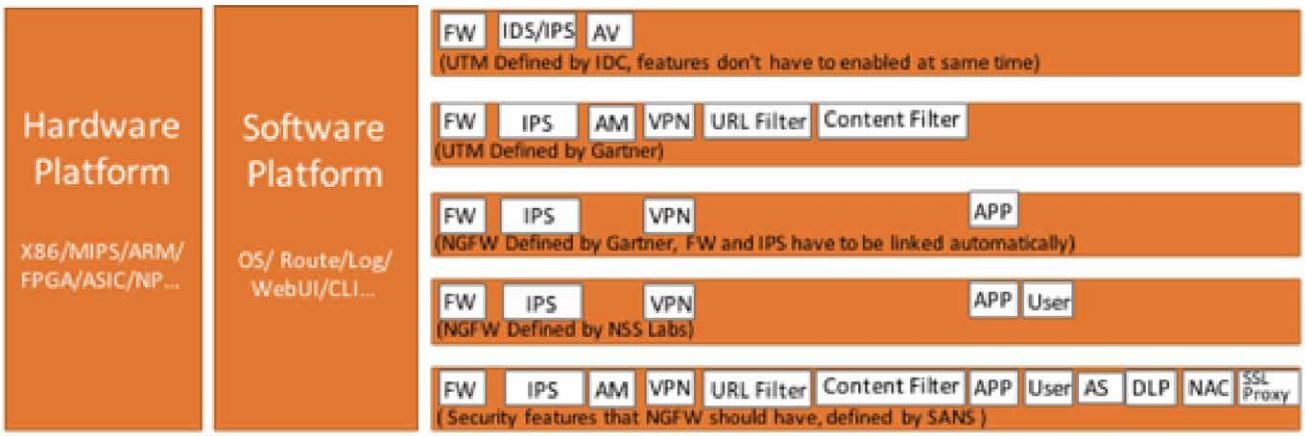



I was extremely excited when we saw monitoring details for cloud applications from the T5060 web user interface. This means that Hillstone has noticed and catered to the current changes in customer requirements. None of the O&M staff will need to stare at interface statistics or URL logs unless there are abnormalities. In reality, they are concerned about service traffic, especially cloud applications. How many people today use this category of applications globally? How much bandwidth do they consume? What are the specific applications? All of these are precious data that may offer valuable O&M guidance. Now, it's frequently found a device claims to recognize hundreds of thousands of applications, which is not meaningful in and of itself. This is because there are typically only a handful of business-critical applications. And it is really valuable to protect and optimize these applications, versus all applications.

We can see that Hillstone has made a great effort to strip away cloud applications. There is still some room, however, to optimize specific details. For example, cloud applications contain both bandwidth-consuming applications such as online storage and applications such as SourceForge and GitHub that don't impose a higher demand on bandwidth but are extremely sensitive to latency and jitter. As their usage scenarios differ dramatically, the policies on the devices are different, accordingly. From an O&M-friendly angle, we hope Hillstone will offer a more granular definition by the cloud application model at the signature library level in the future.

## Intelligence = Data Analytics

Essentially, the transformation from traditional firewalls to the next-generation firewall is a natural evolution for security gateways in terms of passive defense. In 2011, We analyzed the similar product modality in the research "Race with the Next-Generation Firewalls," which clearly shows the process of building security blocks. Although four years have passed, there are no significant changes with the diagram. Many emerging features at that time were not generally recognized by users. For example, now no user will dare to use the hyped "sandbox" for gateways .

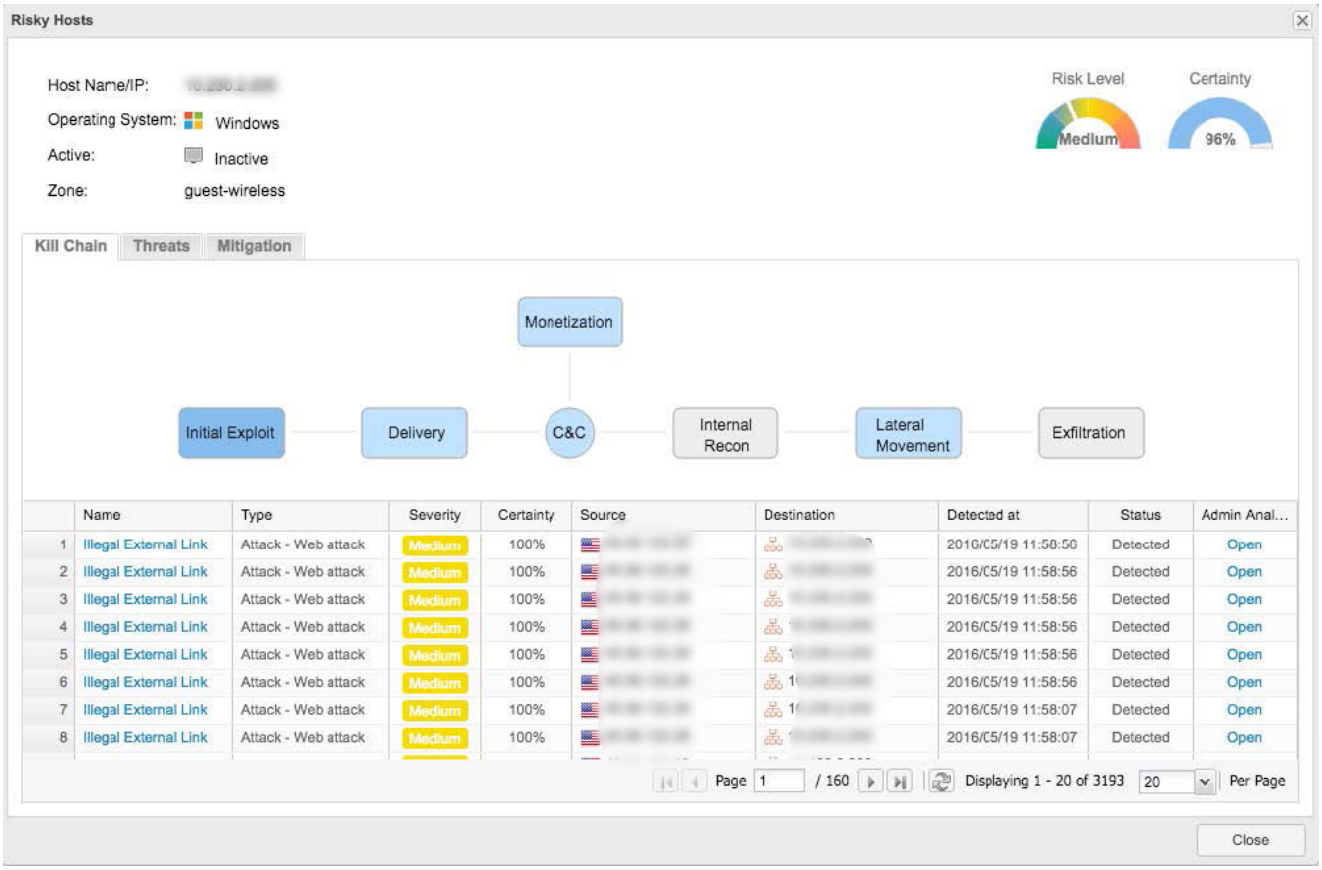



On the one hand, there hasn't been any revolutionary technology in passive defenses for a long time. On the other hand, proactive defense based on data analytics is now becoming more evident to users. Technologically, proactive defense is similar to SoC to some extent in the sense of giving greater prominence to changes in security protection (especially with benefit from "big data"). It focuses on defining security events through behavioral models based on information correlation, in order to provide protection. It doesn't simply supersede passive defense. Ideally, it should be an integration with traditional passive defense. The effect is "1+1>2," which has been regarded as the right direction.

However, as it is too expensive for many enterprise users to comprehensively implement this successfully, they have difficulty in realizing its benefits. Hillstone has made great strides in achieving proactive defense features to some degree based on devices with its T-Series, providing additional value for customers. Simply put, in addition to providing features for the next-generation firewalls, the T-Series is also comparable to a SoC platform except that all the data is collected from various modules in the product. In fact, this involves a lot of engineering. In doing so, Hillstone has added dedicated storage and computing resources to the T-Series to handle the massive data analytics.

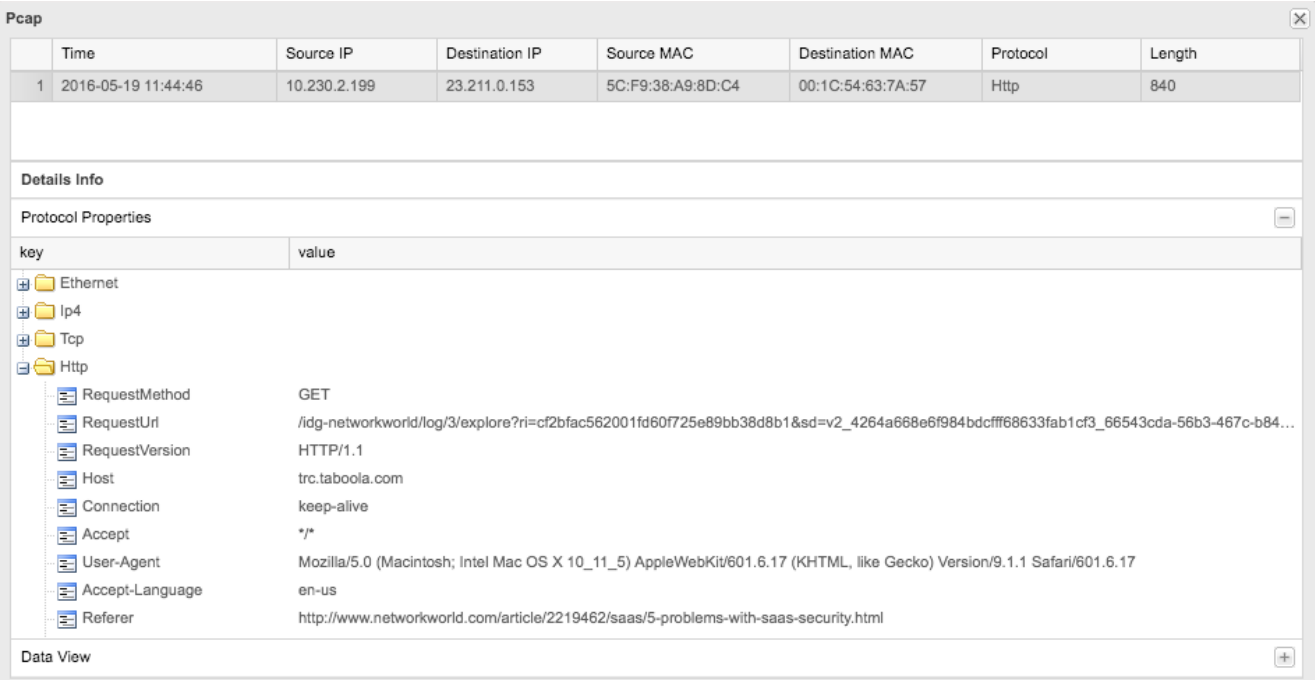
After some time testing the solution, we feel the T-Series offers proactive defense in three areas. First, it helps you see more; second, it helps you understand the context of attacks; and, last, it helps you gather evidence, if needed.

In addition to legacy intrusion prevention and anti-virus, the T-Series also integrates features such as abnormal behavior detection and advanced threat detection. In brief, it monitors the traffic comprehensively in order to provide detection results in different dimensions at different levels. Let's take a figurative example: airport security inspection has activity bursts and even requires human physical pat-downs in addition to the X-ray inspection during specific circumstances or times. After all, combined together , this can provide better security and protection compared to a single security dimension with the X-ray inspection.




However, the cost and complexity of correlation increases with more information. Specifically, with the massive volumes of information in iCenter – the unified event presentation interface within the T-Series – can be overwhelming. Hillstone may also have recognized that and added the "kill chain" to its new version. This is a very creative feature. Generally, devices correlate all the warning information by the spread/breakout process of security threats in the dimension of an IP. Luckily (or unluckily, in essence), they can even reproduce an intrusion behavior completely for O&M staff. I think, this is both the most powerful part of the T-Series as well as what distinguishes it from the competition. It truly has data "say". So, users don't have to engage or add more cost to the function.

After adding engines such as abnormal behavior detection, the T-Series offers the idea of "certainty factor" for threat events, which should be analyzed by the O&M staff. They can define the factor only by backtracking the original message thread when the information collected alongside the "kill chain" is not sufficient to make the judgment call. With an independent large storage capacity, the T-Series can record the evidence and contextextual message thread in real time for security forensics. I believe this is also a must-have for security functions in the era of proactive defense from the perspective of IT systems and compliance.




Generally, the three additional values with the T5060 are three aspects of "seeing" – visibility – at different levels. The "See" represents value in and of itself. At least, without analysis by the T5060, we would never know a business-critical system in the network was the critical unsecure host since it produced more alarms than the sum of alarms against other hosts. Similarly, we cannot know there are many abnormal behaviors on the hosts between the office network and the production network without this analysis. Although it is impossible and even unreasonable for the devices to handle the unknown traffic directly, the T5060 gives us clear prompts so that we can engage in a more targeted manner. We think this truely embodies the value of the feature. We remember when Hillstone named the T-Series the "intelligent Next Generation Firewall." It made the media, users and even competitors think: "I don't know what iNGFW is, but it seems iNGFW is great." They thought it to be powerful. How is it "intelligent"? You can only truly experience that after using it. By its nature, there are root causes for it being "intelligent."

## The following is a real use case:

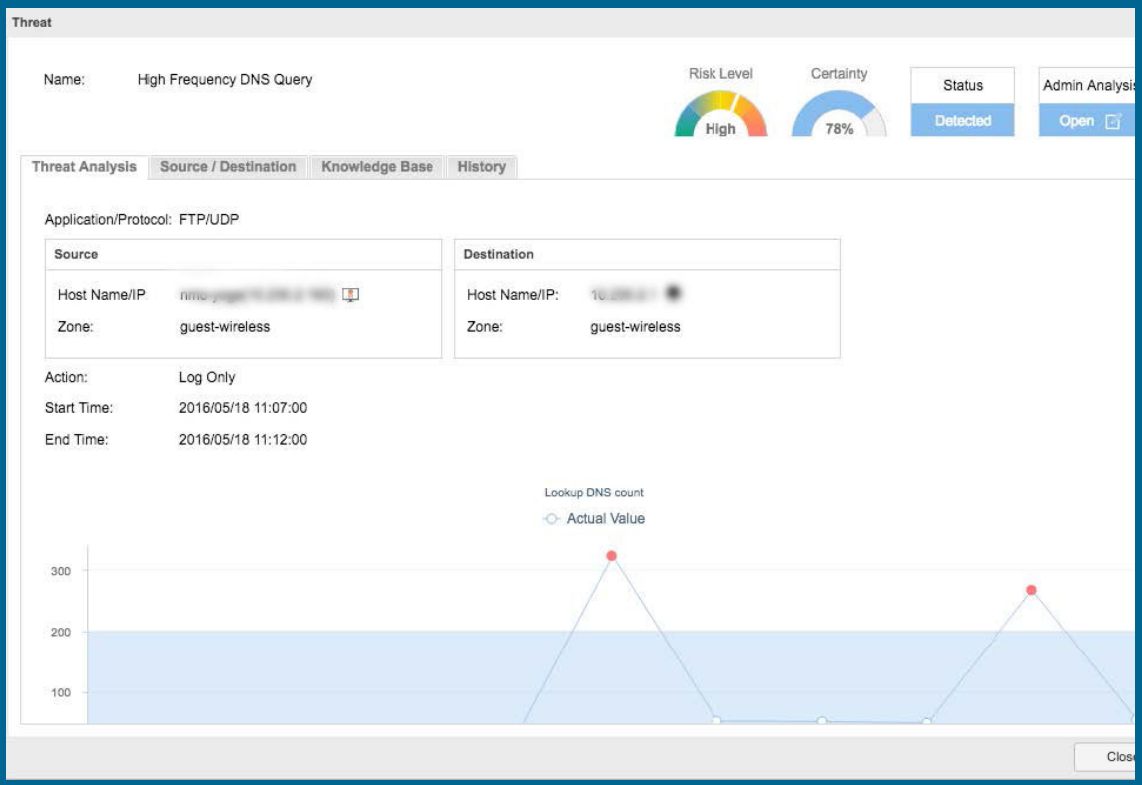
Recently, China Telecom launched DNS resolution protection to disable IP addresses that send more than 50 resolution requests per second for five consecutive minutes. In terms of the traffic model, most small and medium-sized customers will not be affected since their DNS resolution frequency are not likely to go beyond 50. For enterprises, however, one R&D command may disrupt the company-wide network.

But even the IT O&M staff have to recognize the practice of China Telecom. Just as an employee at China Telecom stated, a customer once sent more than 200,000 resolution requests per second to their official DNS, and since the frequency was not limited, which degraded their DNS responsiveness by 90%, thereby affecting all the customers across the network. Although DNS protection policies may affect individual users, it can help guarantee the reliability of most users. It is indeed, worthwhile.

But it is really painful for R&D companies or the network admins for incubator organizations. There tend to be thousands of IP addresses on the intranet during any given peak time. The IP is closed by the official DNS from time to time. Most importantly, it is hard to find a viable solution at a low cost.


The T5060, however, surprised me. The abnormal behavior detection engine will detect the higher DNS resolution frequency and presents it in the summary threat report on the iCenter as a threat event. Obviously, the behavior is not an all-or-nothing action. So, the device may provide the certainty factor for each event based on information such as the frequency and the aggregate. The legacy passive defense features may detect and solve rough attacks against Port 53 on the DNS server (such as UDP Flood). Additionally, attacks such as random domains and native retrospective references can also be discovered by the abnormal behavior detection engine and listed in the report from the DNS server. An integrated judgment is required for the O&M team. For that reason, matrix-based visibility in a specific business dimension is a mandate for them, but is not provided by most tree logging/information presentation devices.

Certainly, visibility is just the first step. We eventually need to solve actual problems; otherwise, it’ s of no value to simply present them. This becomes much simpler with the T5060. You can directly deny behaviors when the certainty factor is 100%. For Flood behaviors with a certainty factor lower than 100%, you can mitigate them directly on the T5060. Mitigation mechanism means delaying a behavior when you cannot determine whether it is authorized or not. As such, the affected user may feel the impact, but other users will not be affected. Even in extreme cases, the T5060 can guarantee DNS services on the intranet (nearly comparable to the network) by completely sacrificing individual terminals. In that case, the solution is very similar to the DNS protection mechanism deployed by China Telecom.




Small problems may cause big issues without the T5060. All the tested next-generation firewalls fail to solve this issue except for the T5060. In addition, there is no function module that dares to regard DNS resolution as a characteristic of unauthorized events in an all-or-nothing passive defense. In an era where attack and defense technologies are exploding and security boundaries are increasingly blurred, the proactive defense and mitigation features of the Hillstone T-Series will play a greater and indispensable role.