Hillstone T-Series Intelligent Next-Generation Firewall Whitepaper: Abnormal Behavior Analysis

Keywords: Intelligent Next-Generation Firewall (iNGFW), Unknown Threat, Abnormal Parameter, Abnormal Behavior, Abnormal Behavior Analysis, Baseline and High/Low Thresholds, Statistical Analysis, Correlation Analysis, Denial of Service (DoS), Distributed Denial of Service (DDoS), HTTP DoS Detection, bandwidth exhaustion, resource exhaustion.

Abstract: This paper describes the Abnormal Behavior Analysis capability of the Hillstone Intelligent Next-Generation Firewall (iNGFW) product. This technology offers a cutting-edge method of detecting unknown threats by analyzing user and server traffic, tracking a myriad of traffic parameters, and correlating and comparing the gathered data to limit risk and reveal potential new threats in advance. Over a period of system learning, each tracked parameter generates a baseline, as well as high and low thresholds. Subsequent behavior patterns violating these thresholds are deemed abnormal and the system generates a threat warning. The correlation of time, parameters exhibiting abnormal behavior, through graphic displays and system warnings enable you to recognize and prevent potential new threats in advance of them impacting your network operation or applications. Abnormal Behavior Analysis is particularly well suited to HTTP and application-layer attacks.

1 Overview

With the rapid growth of network information technologies and network size, business applications for enterprises and government agencies are continuously under attack by increasingly creative and sophisticated methods. Attacks are perpetrated by many different interest groups pursuing a variety of goals ranging from monetary gain, to service disruption, to actions in support of special-interest or political ideologies. Firewalls based on predefined signature libraries cannot prevent new "never-before-seen" attacks until a specific intrusion protection signature that understands the method of the attack is added to the detection database. This retroactive attack detection no longer meets current business requirements.

Firewalls effective in modern business environments must have the intelligence to detect unknown threats before they happen by providing warnings of behavior patterns that may indicate the footprint of a new attack. This unique method of Hillstone's Abnormal Behavior Analysis offers a risk-based security solution. The solution associates user behavior with their traffic, detects user-related behavioral abnormalities appearing over time by comparing traffic to a behavioral baseline, and customizes user-behavior models based on observed traffic patterns. All these capabilities help detect both known and unknown threats from L3 to L7.

2 Threat Management: Network to Application Layer with iNGFW

The iNGFW product implements a security protection concept based on risk factors associated with trackable objects such as applications and users. iNGFW expands the seven-tuple concept of the NGFW product to introduce an eighth tuple – application and user reputation – to the firewall's network security protection capabilities.

Abnormal Behavior Analysis technology analyzes traffic by continuously scrutinizing data flowing through the firewall device. Abnormal patterns in traffic, user behavior or application behavior are detected using various techniques including statistical analysis, correlation analysis and machine learning. Behaviors are considered abnormal relative to historical baselines and thresholds of comparable traffic, users and applications.

Abnormal Behavior Analysis technology involves two important concepts:

- Abnormal parameters: These behavioral parameters at the network layer enable the network administrator to perform multi-dimensional detection of threats.
- Early warnings: Parameter abnormality analytics are used to detect, predict and prevent unknown threats.

2.1 Abnormal Parameters

The iNGFW product gathers data and performs statistical analysis on traffic associated with a variety of target objects. The historical data is analyzed to provide measurements and characterization of dozens, sometimes hundreds, of different parameters.

2.1.1 Types of Parameters

Examples of the types of parameters scrutinized for abnormal behavior include:

- The number of well-known ports used by inbound/outbound sessions
- The average number of transmitted/received packets in active sessions
- The number of new inbound/outbound sessions per second
- The number of active inbound/outbound sessions
- The number of bytes received on inbound/outbound sessions per second
- The number of packets received on inbound/outbound sessions per second

2.1.2 Parameter Baselines and Thresholds

For each monitored parameter, the iNGFW system performs statistical analysis on preprocessed historical data to obtain current baseline, high and low thresholds of normal behavior, defined as follows:

- A baseline refers to a value generated after machine learning over a given period of time.
- High and low thresholds refer to critical values bounding the range of normal behavior. Behavior violating these boundaries is considered abnormal and generates a warning.

Three severities of warnings are issued by the system: low, medium, and high. The severity of a warning reflects the level of deviation between the observed value and the high and low threshold boundaries.

2.1.3 Visually Managing Abnormal Parameters

The management console of the iNGFW product graphically presents the details of each threat, and the abnormal parameters associated with the threat, in the risk management center (the iCenter). Figure 1 shows an example graph of active inbound sessions. A warning is generated when the observed value violates either the high or low thresholds of the parameter.

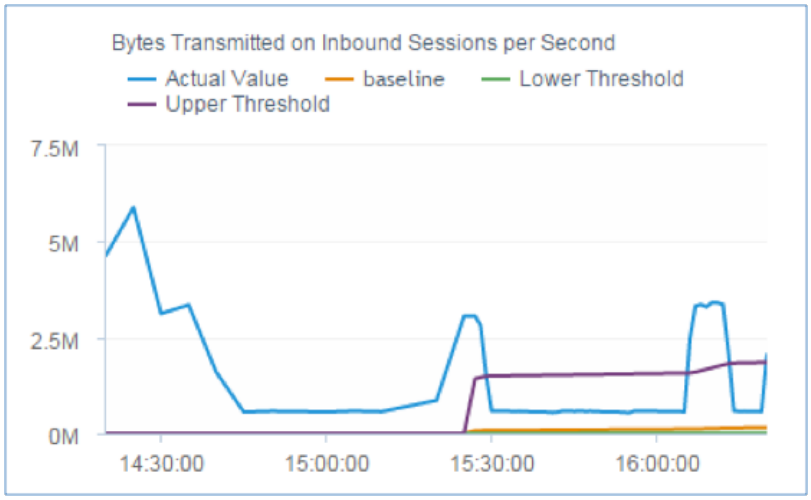

Figure 1: Details of Abnormal Behavior: Active Inbound Sessions

2.2 Early Warnings

There are two techniques for determining whether an early warning should be issued based on observed traffic behavior:

- Statistical correlation analysis
- Determining the source and destination of abnormal behavior to prevent DoS attacks

2.2.1 Correlation Analysis

Abnormal behavior of a single parameter often does not constitute a threat. A higher level of risk is associated with multiple parameters exhibiting abnormal behavior simultaneously. The iNGFW system correlates the behavior of different individual parameters over time to determine whether a new threat may be present, and triggers a warning when behavior is considered abnormal. While individual abnormal behaviors may indicate a random attack attempt, warnings issued based on this detection may be regarded as a "false positive". Detection of abnormal behavior in a set of associated parameters is a more convincing indication of a high level of risk of a potential threat.

The approach of correlation analysis defines rules with various constraints, such as a set of parameters, the types of warnings for these parameters, and the sequence (in time) of warning generation. The approach establishes a correlation between observed abnormal behavior by matching the rules and triggering a warning when a match is found.

Warnings can be categorized into two types:

- Warnings pertaining to attackers or victims, as seen from the perspective of action objects
- Undefined, low, medium, or high warnings in terms of risk level

2.2.2 Source and Destination Analysis

Abnormal Behavior Analysis discovers traffic threshold violations in different dimensions through multi-dimensional observation and comparison of historical traffic. The analysis subsequently locates the source and destination of the violations by backtracking through the data. This approach is ideally suited for detecting traffic abnormalities such as DoS/DDoS attacks, DoS attacks at the application layer, as well as detecting unsolicited bulk message (SPAM) and scanning attacks.

2.3 HTTP DoS Detection

2.3.1 HTTP DoD Detection with Network Layer Behavior

Application layer DoS (also called Hypertext Transfer Protocol, or HTTP, DoS) is extremely damaging to leading service providers and companies doing business over the Internet. There are three aspects to the disruptiveness of DoS attacks: ease of launch, difficulty in filtering and profound impact.

It is not necessary for an attacker to hijack a large number of puppet machines to launch an attack. Instead, the attacker can use port scanning applications to locate anonymous HTTP or Socket Secure (SOCKS) agents across the Internet. Once these are found, the attacker launches HTTP requests to the attack target via the anonymous agents. The attack enters the target website in the HTTP layer by imitating web requests from normal users. In addition to slowing down the front-end webserver under attack, the attack may also impact the back-end business logic servers because the "fake" HTTP requests from the webserver cause an overload of downstream Java, database or logging service requests.

The protection features of traditional firewalls cannot defend adequately against modern DoS/DDoS attacks. More importantly, management and control are unavailable for unknown attacks.

Abnormal Behavior Analysis can perform analysis and detection based on different roles, for example, victims and attackers. For example, for a victim role, the parameters for (i) the number of new inbound sessions, and (ii) the number of active HTTP sessions, may violate their respective high thresholds for a given period of time (say, 120 seconds). If both parameters exhibit abnormal behavior at the same time (correlated), an HTTP DoS warning is generated. In a different approach, correlated abnormal behavior in a set of other parameters may also indicate an HTTP DoS attack, and a warning is also issued when this correlated anomalous behavior is detected.

Figure 2 shows a graph of new inbound sessions. Figure 1 showed a graph of active inbound sessions. The clear correlation between anomalous behavior observed in both these parameters during the same timeframe may indicate an attack.

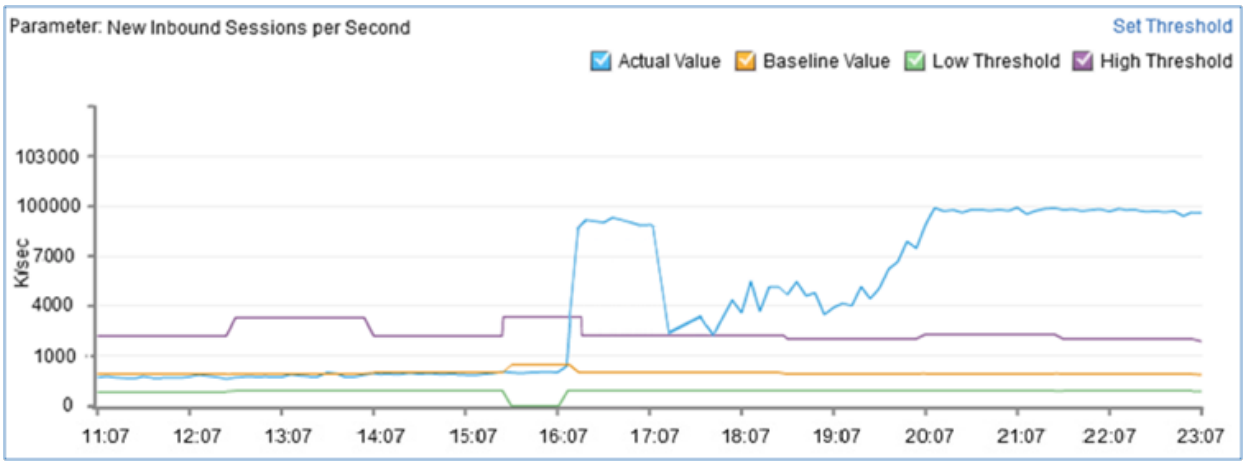

Figure 2: Details of Abnormal Behavior: New Inbound Sessions

2.3.2 HTTP DoS Detection with Application Layer Behaviors

Application DDoS attacks can be categorized into two major types:

- Bandwidth Exhaustion: The goal of a bandwidth exhaustion attack (such as HTTP Flooding) is to consume the bandwidth of the target network by sending a large volume of legal HTTP requests to prevent normal users from being able to access the Web. The attack can be launched in different ways. The attacker sends a large number HTTP requests to the target Web server in a single or in multiple threads. These requests may be generated randomly, or by intercepting normal user request sequences and replaying them. The attacker may request from the Web servers normal web pages (such as a homepage), redirected pages, header information, wrong documents, or send more complicated dynamic content or database queries. The attacker can even simulate a search engine to perform a recursive search, for example to search recursively through all access links on a website starting from a given HTTP link. This latter method is also called spidering.
- Host Resource Exhaustion: Unlike HTTP Flooding, the goal of a host resource exhaustion attack is to deplete the resources (such as CPU, memory, or sockets) of the target host. The attacker requests the Web server to return large files (such as images or video files), or run complex scripts (such as compound data processing, cipher calculation and authentication algorithms) with a few HTTP requests. This method is stealthier because it can exhaust host resources rapidly without requiring a high attack traffic rate.

Application-layer DoS attacks are more destructive and more difficult to detect and prevent than traditional DoS attacks. Therefore, user-based Behavior Analysis offers a superior means of building a dynamic and adaptive access model to protect the target hosts, and to observe network anomalies from multiple angles. Once abnormal behavior is detected, Behavior Analysis identifies and blocks the attack sources.

Building a normal access model requires a period of learning, a process that should be automated without user intervention. The learned results, i.e. the parameters of the access model, are subsequently allowed to be modified by administrators. If a parameter is modified by an administrator, it requires no further learning because an administrator has the highest privilege setting. Manually modified parameters maintain values set by the administrator until they are modified again, or set to "Automated".be modified by administrators.

If a parameter is modified by an administrator, it requires no further learning because an administrator has the highest privilege setting. Manually modified parameters maintain values set by the administrator until they are modified again, or set to "Automated".

Scanning attacks, automated attack attempts, DDoS and Spider attacks all have unique characteristics, a behavioral fingerprint different from normal access. By quantifying the dimensions and parameters of an application protocol, the Abnormal Behavior Analysis model can detect these differences and identify "normal" from "abnormal" behavior.

3 Conclusion

The iNGFW provides Abnormal Behavior Detection technology significantly different from the technology used in traditional firewalls and firewalls based on signature detection. Signature-detection firewalls use a static detection technology that can only detect threats already known within its database of signatures. In contrast, Abnormal Behavior detection is a dynamic technology that builds a model of traffic and behavior parameters based on the collection and analysis of historical traffic, enabling the iNGFW also to detect unknown threats.

The behavior baseline can be adjusted dynamically based on time and parameter thresholds to provide early warnings. These warnings alert the administrator to unexpected or abnormal traffic patterns and can help prevent unknown threats before they happen. Abnormal Behavior Analysis technology reduces operational risk in corporate network services and ensures critical business continuity.

Hillstone NETWORKS

292 Gibraltar Drive, Suite 105, Sunnyvale, CA 94089

Tel: 1-800-889-9860

Email: inquiry@hillstonenet.com

Stay Connected