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 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.
2 Threat Management with the iNGFW Product

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-element concept of the NGFW product to introduce an eighth element – application and user reputation – to the firewall’s network security protection capabilities. iNGFW takes advantage of the Network Health Index (NHI) and Behavior Reputation Index (BRI) scores based on big data analytics to provide intelligent and proactive network protection strategies.

2.1 Proactive Detection with Abnormal Behavior Analysis

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 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.

2.1.1 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. 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

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, middle and high. The severity of a warning reflects the level of deviation between the observed value and the high and low threshold boundaries.

The management console of the iNGFW product graphically presents the details of each parameter. 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 for the parameter as shown between 16:07 and 22:07, with a large spike between 16:07 and 17:07.

![Figure 1: Details of Abnormal Behavior: Active Inbound Sessions](image)

### 2.1.2 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

#### 2.1.2.1 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, middle, or high warnings in terms of risk level

2.1.2.2 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 to 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.

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.
2.2 Threat and Risk Quantification

The Behavior Reputation Index (BRI) measures the health and risk level of each trackable object, such as a user, server or service.

2.2.1 Relationship Between Abnormal Behavior Analysis and BRI

The Behavior Reputation Index (BRI) provides a single quantifiable score of the risk level of an intranet object. This score pertains to every kind of threat:

- **Known threats** are detected through Intrusion Protection (IPS), anti-virus and uniform resource locator (URL) filtering methods. Known threats associated with intranet objects are incorporated into the BRI score.
- **Unknown threats** are detected through Abnormal Behavior Analysis. Abnormal behavior observed in tracked parameters result in varying risk levels which are incorporated into the BRI score.

2.2.2 Rules for Customer BRI Scoring

Using a BRI score, administrators may focus on the most dangerous targets and most relevant behaviors, concentrating their efforts on handling critical threats. Administrators can handle abnormal behaviors detected by the system, but which are of lesser operational importance, by using various actions such as:

- **Excluding certain parameters or behaviors**: Manually excluded abnormal parameter(s) or behavior(s) – these will no longer be incorporated in BRI scoring.
- **Adjusting thresholds**: High and low thresholds can be manually adjusted depending on conditions. When an administrator has more information available than is contained in the machine learning of a parameter’s behavior, they can manually override the thresholds to better reflect a real situation.
- **Reduce sensitivity to “false positives” or “false negatives”**: An administrator may regard a particular warning as a “false positive” or “false negative” in their network. They can adjust the sensitivity of the BRI score to these “false positives” and “false negatives”.

The sensitivity setting ranges from 1 to 9:

- “1” indicates a low sensitivity and relaxes the initial threshold to reduce “false positives”
- “5” is the default sensitivity and indicates the initial threshold
- “9” indicates a high sensitivity and tightens the initial threshold to reduce “false negatives”

3 Conclusion

The iNGFW system provides users with two indices:

- The **Network Health Index** (NHI) quantifies the overall network runtime status, including business services, security risks, device resources and network availability.
- The **Behavior Reputation Index (BRI)** measures the health and risk level of each trackable object, such as a user, server or service.

With these two indices, administrators can proactively manage the hotspots in the system.

Abnormal Behavior Analysis associates network health with risk. The method generates a behavior baseline by adaptively learning the behavioral patterns of dozens of different traffic parameters, as well as correlating the behaviors of the different parameters.

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.