中英文双语

揭秘下一代智能防火墙

Demystify Intelligent Next-Generation Firewall

Hillstone NETWORKS

作者：刘向明

作者简介

刘向明博士是 Hillstone Networks 的创始人之一，现任 Hillstone Networks 首席技术官。刘向明博士 13 岁进入中国科技大学少年班，是 1983 年最年轻的中国本科生之一。在中科大获得物理学学士后，刘向明获李政道中美联合物理招生（CUSPEA）奖金赴美攻读博士，并获得美国得克萨斯州立大学奥斯丁分校物理学博士学位。在从业的 20 年间，刘向明博士曾在美国 Intel, Convex Computers 等著名公司担任研发和管理要职。在创办 Hillstone 之前，刘向明先生曾在 Netscreen Technologies 和 Juniper Networks 担任高级研发管理，负责安全产品的设计和开发。刘向明博士拥有 10 余项国际、国内安全技术专利。

揭秘下一代智能防火墙

Demystify Intelligent Next-Generation Firewall

英文原作：刘向明
中文翻译：侯汉书

Contents 目录

Evolution of Firewalls

Firewalls have been one of the most important building blocks of enterprise security infrastructure for almost three decade. During this time, firewalls evolved through several generations. The first generation is packet based firewall and they exist even today as ACLs (Access Control Lists) in network switches and routers. Packet based firewalls inspect individual packets and packets are filtered by simple matching of fields in the Ethernet and IP header. No state information of protocol or application is maintained. For example, in Cisco ACL implementation, there is a primitive TCP state check using an "established" keyword to restrict the flow of SYN packet. Today, packet based firewall only exists as a function in network devices where resources are limited, and high throughput is of utmost importance.

In the 1990s, stateful inspection firewalls were introduced. Most stateful inspection firewalls operates on the layer 3 and 4 of OSI. In these firewalls, flow state called "sessions" is introduced to keep track of open connections. The session is identified based on the 5-tuple (source and destination IP and port, IP protocol number). Sessions allows for maintaining bidirectional conversation even when unidirectional policy is used. For example, in a scenario where nobody from outside of the company can initiate connection to the inside, traffic from someone outside (Bob) is allowed to reach someone inside (Alice) only if Alice initiates the connection to Bob first.

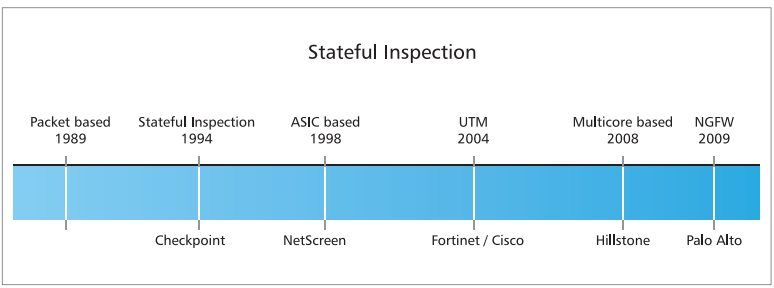
Sessions are also used for maintaining other layer 3 and 4 information such as TCP state and NAT translation information.

Besides maintaining sessions, stateful inspection firewalls also need to understand a few application protocols. Some applications (e.g. FTP)

open up connection on the fly with dynamically selected TCP/UDP ports, other applications such as VOIP protocol may open connections with a third party. In order to maintain application usability under the circumstances, stateful inspection firewalls support Application Layer Gateways (ALGs) that inspect the content of the application protocol and dynamically generate temporary rules to allow these connections to establish.

With firewall staying on the network layer, application security demands drove the appearance of security products such as IPS, Anti-Virus, URL filtering. Unified Threat Management (UTM) is a security appliance that combines stateful inspection firewall with these application security features.

Recent years saw the rise of next generation firewall (NGFW). With stateful inspection firewall controls network traffic based on IPs and ports, NGFW use deep packet inspection (DPI) technology to look inside protocols and contents to classify traffic. Modern day HTTP can carry a variety of types of traffic, from web surfing, business application, social networking, multimedia, P2P download and even malware and attacks. NGFW decodes protocols and contents and typically use a combination of pattern signatures and behavior signatures to identify application. Policies on NGFW rely on 7-tuples match: IP 5-tuple, plus application ID and user ID.



Paradigm Shift in Security Methodology

Threat Based Security vs. Risk Based Security

During the past few years, we have seen increasing number of high profile security breaches from fortune 500 enterprises and government. Part of it is due to new regulation. Security and Exchange Commission (SEC) in 2011 issued guidelines that public traded company should disclose security risks and incidents in financial statement, especially those that have a material effect on their operations. With the likes of Google, Intel and RSA announced they are the victim of security incidents, more and more companies are willing to "come out of the closet". Any company with internet access is highly likely to face cyber-attacks at some point in time.

So if all these large named enterprises cannot fully defend against these attacks, what does it say about the other companies who do not have such large amount of resources available to them?
Do you have enough network security? Do you need to have that latest piece of security hardware to defend against a specific threat? The key to answer this question lies with understanding the risks.

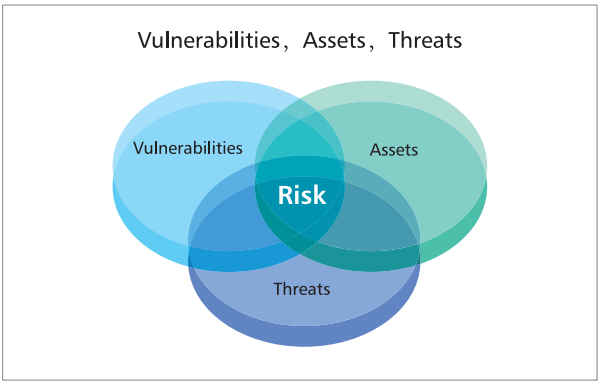
A threat based security model identifies types of threats we are trying to protect against, then device specific defenses against these threats. In the past, for transmission of virus and Trojan files, we have Anti-Virus solution. For network based attacks against applications, we have Intrusion Detection and Prevention (IDS/IPS) solutions. To defend against a new kind of attack, we add an IPS signature to the signature detection database.

The problem with this approach is the defense is effective if the attacks

can be clearly understood. With the proliferation of zero day attacks and APT, this no longer holds true. New techniques emerges that looks at patterns in the traffic for behaviors that indicates whether an attack is undergoing.

A risk based security model is one that device security protection of company's IT infrastructure and assets based on risk analysis. So what is risk?

Risk = Asset x Vulnerability x Threat



Risk is the intersection of Asset, Vulnerability and Threat. Asset is what we are protecting that is of value. It can be real assets like money or property. Or it can be assets like credit card files, source code, web sites, company reputation etc where the lost or compromise of these assets may cause intangible damage. Vulnerabilities are holes that can be exploited to gain illegal access to the assets. These include physical infrastructure such as unprotected network and unpatched software, as well as human factor such as employees who are not security aware. Threats are what we are protecting against. These are means to exploit the vulnerabilities such as network attacks, Trojan email etc. Asset, Vulnerability and Threat forms the essential elements of risk and without any one of them there is no risk.

Threat based solution only looks at the threat dimension. In many

solutions, only known threats are dealt with. A risk based solution deals with assets. Both known and unknown threats to assets, as well as vulnerabilities of the assets are considered.

In a risk based security model, you should invest in security protection in proportion to the risk. You should invest in security protection in proportion to the value of assets you are trying to protect, and in proportion to the damage that you suffer if the system is breached. Take a home security analogy, for a regular home, a regular door and lock suffice. But if you regularly have a stash of cash at home, you would buy a safe. Furthermore, if you have arts and crafts at home that worth a lot of money, you would invest in a home security system. An increasing number of hackers are driven by money rather than political reasons. For these hackers, if the resource put into the hacking is higher than the potential return, they would be reluctant to carry out the attacks.

Following risk based security methodology, an enterprise can evaluate risk before incident happens. Security measures can be implemented proactively by increasing defense for high valued assets and where threats and vulnerabilities are the most serious. And when risk level changes because of newly discovered threats and vulnerabilities, security policies can be adjusted dynamically to secure critical assets.

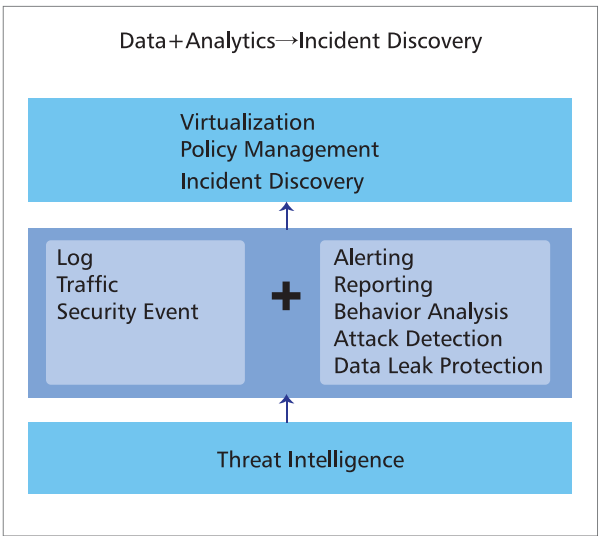
Security Analytics

Traditionally network security products are threat centric. We incorporate security mechanism in reaction to the threat we are facing. These security mechanisms are usually signature based. When a new attack is discovered, the traffic is analyzed and signature of the new traffic is added to the signature database. The system monitors running traffic for patterns in the signature, and if a match is found, the system flags the traffic for possible attack. Most of the intrusion detection and prevention system today incorporate a signature based engine.

The signature based method is very good at detecting known attacks that are not encrypted. However, there is an obvious drawback that the exploit has to be known in order for it to be analyzed and new signatures

written for it. New kinds of malwares and attacks that are polymorphic, and the growing threat of Advanced Persistent Threat (APT) and the zero-day exploit that they relies on make signature based method grossly inadequate.

APTs and other sophisticated attacks use highly covert measures and leave behind very few auditable events such as logs and events. Some of the auditable logs and events are simply too abundant and does not indicate by themselves serious security incident. But, these attacks, if network based, always leave behind traces in traffic and flow data. Big data analytics can use techniques such as correlation, machine learning to discover traces of attacks that is harder to erase.



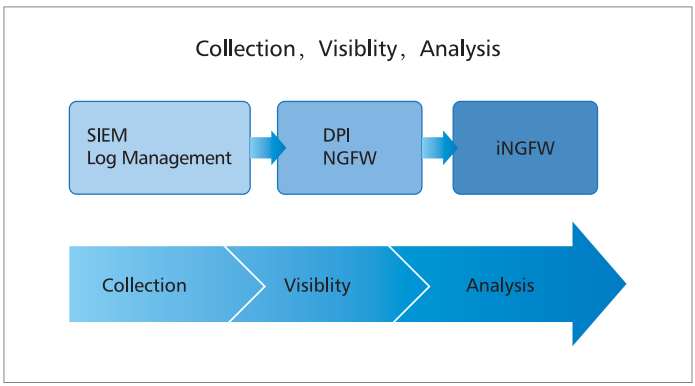
By analyzing of large amount of security data of different type, big data analytics is good at finding out abnormal behavior patterns in the traffic. It is an important contributor to the risk assessment of users and systems on the network. Security measures could be taken to reduce exposure to high risk users and systems and increase monitoring if necessary.

The advance in network computing and big data technology makes it

possible to capture and analyze large amount of security data in real time: syslogs, security logs, session information and packet captures. Flow data and packet captures open up a great wealth of information not available in system and event logs. With this information, a data analytical system can:

- Analyze user behavior
- Analyze application behavior, optimize application performance
- Analyze traffic patterns, optimize network traffic
- Detect data leaks
- Detect botnet in the network

Business has been using SIEM (security information and event management) system for these purposes. SIEM can accept data from many devices and can correlate data across the network. The downside is the analysis is done after the fact and the feedback to the enforcement policy is usually not complete.



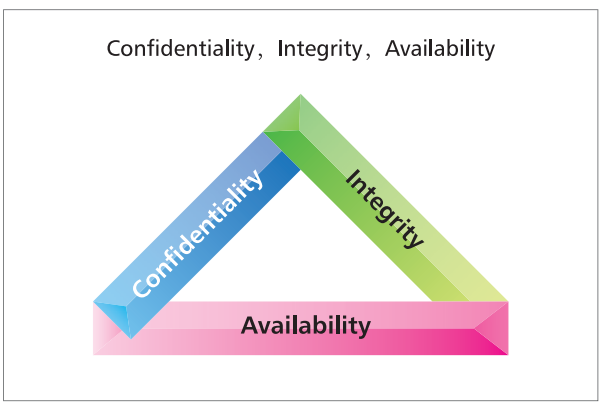
Firewall situates in a critical point of the network in between different security zones. It sees all the traffic for which security enforcement and monitoring are important. Firewall with the evolution to NGFW has started to collect and aggregate traffic and event data and use it for visibility purpose. The latest DPI technology is then able to dissect the traffic into applications and users. Armed with this information and powerful hardware, the firewall can analyze the data in near real time and dynamically change enforcement policy according to changes in the network.

An integrated data analytics solution in firewall has several advantages. First of all it offers best responsiveness. For modern zero-day attacks, there is a time difference between when an attack starts and when it is detected. An integrated solution will minimized this time and able to mitigate the damage. Secondly, an integrated solution can deal with types of real time data not supported on third party analytics solution. A large amount of data can be consumed locally and does not need to be transmitted between devices. Since modern day analytics relies on traffic data which is orders of magnitude more than event data, this has significant impact on viability of the solution. Last but not the least, integrated solution offers a cost advantage, not only during the initial purchase, but also in daily operation by avoiding management of multiple devices.

Security and Availability

There is a well known security principle called CIA triad. It is the 3 components of information security. C in CIA stands for Confidentiality: the data you are protecting must be protected from unauthorized access. I stands for Integrity: the data you are protecting must be guarded against unauthorized modifications.

Beside these two components which prevent unauthorized access and changes, Availability is the key third component that make sure authorized access are allowed and can go through when needed.



Business application and services is the lifeline of today's enterprises. The availability of these application services is critical to the day to day operation and business continuity. Disruption or failure of them can cause grave adverse effects monetarily, and in some cases, to human lives. Recent trend in cloud computing, mobile technology and social networks adds to the complexity of the IT infrastructure. Network itself as the basic element also undergoes rapid changes. Traditionally, enterprises use network management software to monitor the state of network and use server management systems to monitor state of applications. The separation of the two systems offer separate views of the IT operation but has the shortcoming that it does not show the relationship between the usability of the network and the applications. This makes it more difficult to foresee application problems beforehand and pinpoint issues afterwards.

Denial-of-Service (DoS) is one attack that target the Availability side of the security model. But the availability issues in the system goes far beyond just DoS prevention.

- DoS and DDoS attacks: Attacks to the system by making resources or system unavailable for normal usage. There are several types of DoS attacks. Bandwidth DoS attacks by takes up available network bandwidth using large amount of traffic. Resource DoS attacks by exhausting resources on the system such as CPU, TCP connections using targeted traffic that each takes up a large amount of resource. Crashing DoS attacks crash the application or operating system by exploiting software bugs in them. DoS attacks can further be categorized into regular DoS attack where one source systems is used and Distributed DoS (DDoS) where a large number of systems participate in the attack.
- Network devices failures: Failure of the device operation by network device hardware failure of device or links, device software bugs etc.
- Inappropriate network configuration: As the cause of many network failures, traffic errors by routing loops, broadcast storms by improper switch connections etc. falls into this category.
- System failures: Failure of system or application due to server/storage hardware failure, software bugs etc.

- Inappropriate system configuration: Failure or degrade of application service may result if the system or application is not configured properly.
- Bandwidth allocation and application optimization: Even if all system and network operates normally, there can be application availability issue when the traffic changes. For example, video conferencing or VOIP call traffic maybe affected if the volume of P2P traffic increases and takes up all the bandwidth.
- System and Network outages
- Human factors such as inadvertently disconnection of links.

Availability is one factor that has been neglected in the firewall technology. The anti-flooding functionality in most firewalls today address DoS/DDoS problems only and even then are grossly inadequate to prevent modern DoS/DDoS attacks.

Problems with NGFW

NGFW does not have the capabilities to adjust enforce-ment based on behaviors

The bases of Next Generation Firewall are the identification of application, user and content and security control based on the identification results. Policies are configured on firewalls that determines whether the user be allowed to use the application with the content. And enforcement is done based on application, user and the traditional IP 5-tuple (source and destination IP, source and destination port, IP protocol).

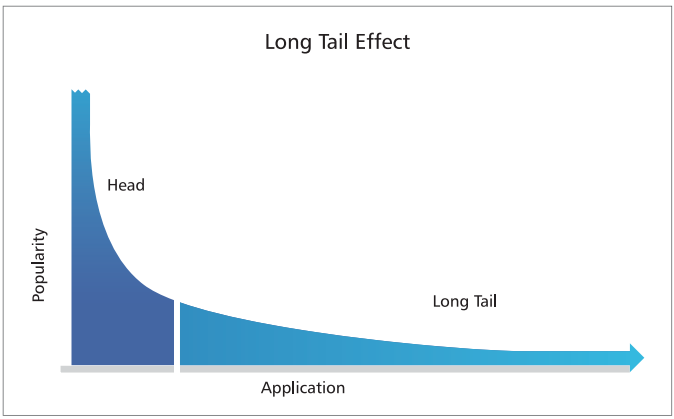
But there may be other factors that affect the acceptable access control

level for a user. Application usage that is acceptable at one time may be suspicious depending on the user or system's history of usage. One factor that should affect user's access level is his risk level, or "reputation". Has the user been doing questionable things such as a higher level of access to websites that contains malware? Has the user's machine shown bot behavior by sending outbound DDoS or contact known Botnet Command and Control IPs? Has the user shown unpatched OS and applications? All these may be reasons to limit the user's access to critical resources. A user's reputation may change over time and so should be the user's level of access.

Let's look at the few elements that contribute to the risk level of the user or system. NGFW does not look at user behavior as a correlation of user traffic usage and other events. Specifically, it does not analyze the information collected along the time dimension. Therefore a user is given a certain level of access and NGFW does not have the capability to adjust that level of access dynamically. The acceptable set of applications may change over time according to risk perceived.

NGFW does not look for abnormality in traffic, either in relation to other similar user or system entities, or through time. For example, a user that does not see much activity for a long time suddenly becomes active, or the responses time and rate of a web server deteriorate dramatically. These are suspicious events that should be investigated. Abnormality in behavior patterns should adversely affect a user's reputation, and proper adjustments to access policies need to be made.

Long Tail of Application



With the growing use of smart phones and Web 2.0, the number of applications increased tremendously. A press release in October 2012 put 700,000 as the number of applications for Android and about the same number for iOS. The number of web application essentially tracks the number of web sites out there. According to a survey by Netcraft in March 2012, there are around 644 million web sites and that number is increasing at a rate of 5% per month. We have not started to count the number of application functions in each web site. However, the number of applications identified by next generation firewalls today ranges from a couple of hundreds to a couple of thousands.

What this means is there are simple a large amount of applications that fly under the NGFW application identification radar. As shown in Figure, the "long tail" represents applications that are less popular and not covered by the application signatures on the firewall. But because their numbers are so high, the total usage of these applications may equal or exceed the total usage of some popular applications.

As a result, policy enforcement may not achieve the desired results. If one desired to block file uploading, traditional firewalls may identity FTP and HTTP based uploads and block them. NGFWs go further by adding more applications such as box.com or Facebook upload. But what about file

uploading programs and websites that falls in the “long tail”? Can they be identified and properly blocked?

Heavy usage of unknown applications increase risks to the system and administrators needs to be alerted. Adjustment to level of access or additional monitoring can be made to these users.

Encrypted traffic

Application identification also runs into problems for encrypted traffic. There are certain types of encrypted transport like SSL and SSH for which it is possible to decrypt the content. For others we have to rely on traffic behavior patterns to identify the application. Those unidentified traffic then has to be allowed or denied as whole, all or none. It is possible to whitelist known applications and deny all the unidentified traffic, but in reality, because of the long tail of applications described above, there are always applications that people use that falls into the unidentified category and get blocked unintentionally. IT support calls will rise and user experience will suffer as a results.

Heavy usage of application that encrypts contents may also affect the risk level of the system. Administrators could also consider different access level or monitoring policy for these users.

Intelligent NGFW

iNGFW is a firewall that use advanced data analytics of security and traffic data and proactive monitoring to deliver risk based security to the customer. Administrators can manage security based on perceived

risks of the networks and assets, and prevent security issues or system outages before they occur. iNGFW's enhanced NGFW features offers comprehensive visibility into network/user/application and dynamic control of policies.

iNGFW implements the following functionalities:

- Proactively monitor network and user traffic. iNGFW uses big data analytics to detect abnormal behavior, unusual system usage and guard against zero-day attacks. Behavior Reputation Index (BRI) is a reputation measurement of intranet users, hosts and services. This allows for visibility of risks associated with intranet assets.
- Proactively monitor availability of resources, network and services, reduce chances of service interruption and downtime. Risk analysis of user, resource, network, application usage and behavior. Network Health Index (NHI) summarizes security and availability issues faced by the system. NHI offers visibility of healthiness of the whole network and each subnetworks.
- Reporting of system risks through BRI and NHI. Alerts are generated when health states of target objects or network change.
- Dynamical adjustment of access control and traffic control policies can be made based on BRI of target objects and/or NHI of subnetworks. Policy control is done using 8-tuple: reputation, IP 5-tuple, Application ID and user ID.
- iQoS that offers fine grained control of user and application traffic, and delivers availability guarantee of critical business applications.
- Visibility of user, resource, network and application usage and associated risk assessment.

Behavior Analytics and Behavior Reputation Index (BRI)

iNGFW collects traffic information through continuous, real time monitoring of traffic going through the device. In the meantime, up to date threat intelligence combined with unified threat detection engine generate security event logs. iNGFW data analysis system processes data from multiple sources in near real time and analyze the risk associated with intranet users, hosts and services. The risk levels of intranet objects

are visible through Behavior Reputation Index (BRI). This risk level can also be used to dynamically affect policy enforcement of these objects.

In the analysis phase, iNGFW first uses application and user identification technology to classified collected data. Each targeted object can be a user, a host or a service. Here behavior of the targeted object is a collection of information relating to the use of information and resources over the network at a specific point in time:

- Traffic Usage:
  - traffic information,
  - bandwidth,
  - application mix,
  - request rate,
  - response time
  - sources accessing this object
  - destinations which this object is accessing
- Attacks originating from the object
- Attacks targeting the object
- System information
  - device information
  - OS version
  - patch information
  - application information (AntiVirus software, downloader etc)

iNGFW introduces a Behavior Reputation Index (BRI) for intranet objects. This index is an indication of the health state of an object and its risk level.

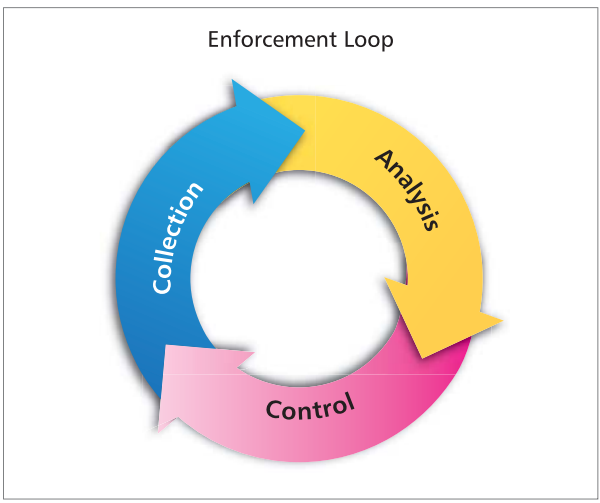
An object’s reputation may depend on several things.

- The current behavior of the object.
- The historical behavior of the object: This maybe a history of attack events, a history of application usage etc.
- The behavior of the object comparing to his peers: A user with usage patterns that is very different from others may raise a red flag.
- The change of behavior of the object over time.

iNGFW then use data analytics technology and machine learning to look

for activities and patterns that indicates problems.

- Whether network and system usage complies with company Acceptable Usage Policy. Heavy use of social and media applications may indicate a productivity problem. Heavy use of unknown applications may be a security breach that needs to be investigated.
- Normal network and system usage compared with historical data. Sudden change of behavior may not always indicate a problem. But there are cases that should be causes of alarm: sudden appearance of new services on web and application servers, sudden burst of activities for dormant users.
- Abnormal network and system usage compare with peers. Top users of non business related application may be causes for investigation, for example, users of P2P or unknown applications.
- Correlation of event log and traffic signature for botnet detection



One thing the data analytics system is good at is detecting data leaks. Usually these kinds of data leaks are accompanied by unusual application usage or abnormal activities. Usually the activity will see the user hitting more servers than normal and may see a higher level of denied access. The user may use a higher volume of questionable application such as downloaders, proxies, tunnels or unknown applications.

Advanced Persistent Threats (APT) are attacks that are more sophisticated, organized and targeted. The activities of an APT attack are well disguised and detection that relies on single events will generate too much false positives to be useful. A behavior detection system that can analyze massive amount of data of different kind can find advanced patterns of APTs that together will give strong indication of attacks.

In depth data analysis can also discover activity of infected systems in the network. The system looks for connection to Command and Control servers and outbound attacks. Early detection of such systems alerts administrators of network breaches and can help limits damaged caused by them.

iNGFW provides risk based security management by offering visibility of reputation of intranet objects in the system. Behavior Reputation Index (BRI) is a measurement of object risks based on the behavior analysis. By concentrating on the top risky targets in the system and the behavior issues found related to these targets, the administrator is able to focus on addressing the most serious problems in the system.

In iNGFW, security analytics can be dynamically feed into security enforcement through reputation based access control. This combination reduces the time between the problem action arises and the remediation.

Proactive Monitoring and Network Health Index (NHI)

One way iNGFW protects application availability and preserves business continuity is through proactive monitoring. iNGFW monitors applications, servers, key nodes in the network and resource consumption through periodic probing. The results of the probing are correlated and analyzed to give an overall evaluation of the health of the network and availability of services. In many cases the deterioration of the condition can be observed and administrator alerted before the service becomes completely unusable. When problem arises, the system also offers a complete report of the health of individual elements. This helps with troubleshooting and shortens the time to pinpoint the failure.

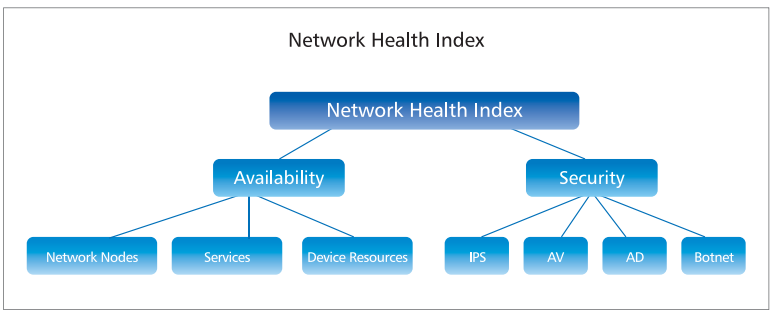
The metrics that can be monitored includes:

- Traffic volume on network links
- Application mix in the traffic
- Packet loss and latency for network devices
- Packet loss and latency for servers
- Request failure and latency for applications and services
- System Resources such as CPU, memory, sessions

The Network Health Index (NHI) is a measurement of the risk that impacts usability of the network and services on the network. NHIs are computed for each subnetwork, either through connected interfaces or security zones. When the health state changes, the administrator can be notified and actions can be taken preemptively.

There are three health states:

- Healthy: Network and service are operating normally
- Subhealthy: Even though the service is not disrupted, there are conditions that potentially could lead to serious issues. The administrators should mitigate the issue and avoid failures from happening. For example, sustaining high CPU utilization or resources near exhaustion.
- Unhealthy: Problems arise that seriously affect the normal operation of network and service.



Network Health Index is an evolving system that evaluates and summarizes the ability of network, systems and applications to deliver expected service for business operations. It is divided into two units, security evaluation and application and service availability.

Security evaluation unit looks at security events and vulnerability in the system to determine existing or potential threats of the system. For the three components that comprised of risk, this unit evaluates the threat and vulnerability of the system.

- Threat state: including threat of attacking others and threat of been attacked
- Abnormal Behavior Analysis: The security data is analyzed for abnormal activities. The abnormality can be in comparison with peers or with historical data.
- Vulnerability Detection: Systems on the network can be scanned for vulnerability. Endpoint agents can also report compliance information about the devices.

Application and service availability unit is supported by three monitoring components: server and application monitoring, network device monitoring and resource monitoring.

- Server and Application Monitoring: Monitor server and application response time
- Network Device Monitoring: Monitor connectivity and latency of network devices
- Resource Monitoring: Monitor key system resources such as CPU, memory, sessions etc.

In general, the health index of a monitoring unit or components is a calculated from the health indices of all of its subcomponents. For each unit, components and subcomponents, there are a subhealthy threshold and an unhealthy threshold. In general, if any one of the subcomponent is in Unhealthy state, the containing components and the whole system is in Unhealthy state. If any one of the subcomponent is in Subhealthy state, the containing components and the whole system is in Unhealthy state. This ensures that local problems are propagated to the top and visible to the whole system.

With each monitoring unit, component, subcomponent having a health index, we can give a health view of whole network. The hierarchical structure of the monitoring component helps administrators to proactively locate and diagnose problem spot.

Aside from resource monitoring, other types of monitoring and security evaluation can be associated with an interface or security zone on the firewall. This is the interface or security zone where the traffic of the monitoring or security events corresponds to. By dividing the networks into subnetworks based on interfaces or security zones, NHI can be computed on each of the subnetworks. For example, if bots are detected in DMZ security zones, the risk level of DMZ is elevated, but not necessarily other parts of the networks. NHI offers a great way to visualize risks level associated with each networks and gives an overall assessment of the health of the network.

Reputation Based Access Control

Based on the Behavior Reputation Index and Network Health Index, the intranet objects and subnetworks are categorized into three health states: Healthy, Subhealthy and Unhealthy. iNGFW uses a reputation based access control that apply access control and traffic control policy based on 8-tuple: health state, 5-tuple IP information, application ID and user ID.

Enterprises can take advantage of reputation based access control and devise different policies for users in different health state. For users in Unhealthy state, the users should be quarantined and may be assigned to a remediation network, or offers access similar to visitors of the network. Users in Subhealthy state may be barred from accessing sensitive or highly confidential resources in the network. As a user-friendly measure, the user should be notified when their access is limited because of their health state, possibly through an endpoint agent or a web page popup. This way they can proactively address the issue by contacting the network administrator.

Similarly, Network Health Index can affect policies between different interfaces or different security zones. Policies can be dynamical changed based on the health state of subnetworks associated with interfaces or security zones.

Both BRI and NHI are dynamical numbers that may change over

time. New attacks or vulnerabilities may be discovered, devices may malfunction that affects availability. When BRI or NHI changes to the point where the health state of target objects or network changes, the level of access can be dynamically adjusted to reduce risks.

BRI and NHI help administrators locate high risk areas and proactively address ongoing and potential problems. Reputation Based Access Control allows administrator to reduce risks by limiting the exposure of sensitive information.

Summary

Highly evasive nature of advanced threats and zero day attacks has made signature based protection more and more vulnerable. The security protection paradigm is shifting from threat based protection to risk based protection. iNGFW is a risk based security solution on top of enhanced Next Generation Firewall. Through continues monitoring, collecting and analyzing traffic and availability data, iNGFW proactively looks for abnormal behaviors and potential network-wide issues that affect network operations. iNGFW offers two indices: Network Health Index is a summary index of the potential security and usability risk of the network and services. Behavior Reputation Index is a measure of health state and risk level of individual intranet objects: users, servers and services. A reputation based access control associates the health state and risk level with the level of access. By dynamic adjustment of access control based on perceived risk, iNGFW helps administrators reduce risk exposure of enterprise network and services.

防火墙演化史

在过去的半个多世纪里，防火墙一直是企业安全基础架构最重要的基石之一，其间也经历了几代的演化。第一代防火墙是基于包过滤的的防火墙，时至今日这类防火墙仍在网络交换机和路由器中以访问控制列表 (ACL) 的形式发挥着作用。基于包过滤的防火墙检查每个报文，并简单的根据 Ethernet 和 IP 头中的字段匹配进行过滤，但不维护协议或应用的状态信息。例如，Cisco 在实现 ACL 时使用“established”关键字进行原始的 TCP 状态检查，限制 SYN 报文流。目前，基于包过滤的防火墙仅存在于资源有限但要求高吞吐量的网络设备中。

上世纪 90 年代出现了状态检测防火墙。大多数状态检测防火墙运行于 OSI 的三层和四层。这种防火墙引入了被称为“会话”的流量状态用于追踪开放连接。会话是基于五元组 (源 / 目的 IP 和端口，IP 协议号) 进行识别的。即使使用的是单向策略，建立起的会话也允许双向流量。例如，假设公司外部员工无法发起到公司内网的会话，但只要内网员工 A 首先发起了到外网员工 B 的会话，B 的流量就可以到达 A。

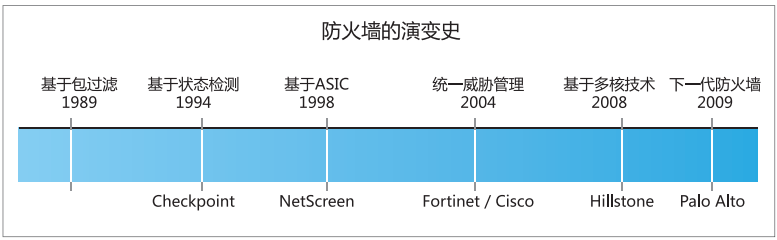
会话还可以用于维护其他三层和四层信息，如 TCP 状态和 NAT 转换信息。

除了维护会话外，状态检测防火墙还需要了解一些应用协议。有些应用 (如 FTP) 在动态选择的 TCP/UDP 端口上打开临时会话，还有些应用 (如 VOIP 协议) 可能需要打开到第三方的会话。为了

在上述环境中保持应用的可用性，状态检测防火墙支持应用层网关 (ALG)。ALG 检查应用协议的内容并动态生成临时规则允许创建这些会话。

网络安全防护对应用安全的需求促成了 IPS、防病毒、URL 过滤等安全产品的出现。统一威胁管理 (UTM) 就是结合了状态检测防火墙和上述应用安全功能的安全设备。

近年来我们见证了下一代防火墙 (NGFW) 的崛起。状态检测防火墙基于 IP 和端口控制网络流量，而 NGFW 使用深度报文检测 (DPI) 技术深入到应用层协议和内容对流量进行分类。现在 HTTP 可以携带各种类型的流量，从网页浏览、业务应用、社交网络、多媒体、P2P 下载到恶意软件和攻击。NGFW 对协议和内容进行解码，通常结合模式特征和行为特征以识别应用。NGFW 的策略基于七元组匹配：IP 五元组外加应用 ID 和用户 ID。



安全方法论的转变

基于威胁的安全和基于风险的安全

在过去的几年里，在世界 500 强企业和政府机构中安全事故层出不穷。出现这种结果部分要归因于新的管理规定更加严格。美国证券交易委员会 (SEC) 在 2011 年发布指导要求上市公司应在财务报告中披露安全风险和事件，尤其是对运营造成实质影响的风险和事件。随着谷歌、英特尔和 RSA 相继宣布他们都是安全事件的受害者，越来越多的公司都愿意公开承认安全事件。任何使用互联网的公司随时都很可能要面临网络攻击。

如果连这些大名鼎鼎的公司都无法完全防御网络攻击，其他没有太多可用资源的公司情况又如何呢？你的网络足够安全吗？必须拥有最新的安全设备才可以防范特定的威胁吗？回答这些问题的关键在于如何理解风险。

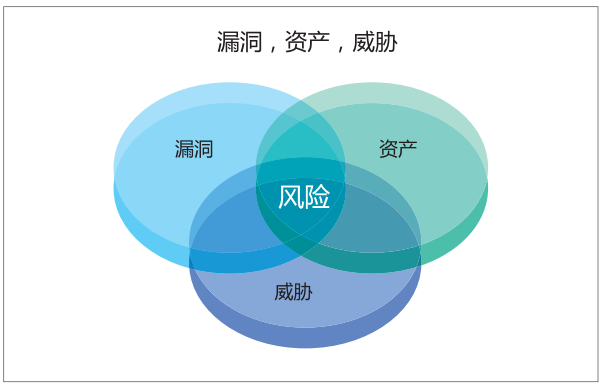
基于威胁的安全模式是先确定需要对哪些威胁类型进行防范，然后设备再有针对性的防范这些威胁。过去，对于病毒和木马文件传输，我们有防病毒解决方案；对于基于网络的应用层攻击，我们有 IDS/IPS 解决方案。为了防范新的攻击类型，我们需要向检测规则数据库中添加 IPS 规则。

这种方法的问题在于只有在充分理解了攻击的前提条件下才能进行有效防御。随着 0-day 攻击和 APT 的扩散，这种方法不再奏效。目前出现的新技术通过在流量中查找行为特征，来判断是

否有攻击正在发生。

基于风险的安全模型指的是基于风险分析对公司 IT 基础设施和资产所实施的设备安全保护措施。那么，什么是风险呢？

风险 = 漏洞 x 资产 x 威胁



风险是资产、漏洞和威胁的交集。资产是我们所保护的有价值的东西，可以是有形资产，如金钱或财产，也可以是无形资产，如信用卡档案、源代码、网站资源、公司声誉等。漏洞指的是可以被利用的获得对资产非法访问的缺陷，如未受保护的网络和未打补丁的软件或没有安全意识的员工。威胁是我们需要防范的东西，如利用漏洞的手段对网络进行攻击、木马邮件等。资产、漏洞和威胁构成了风险的基本元素，缺少其中任何一项都不存在风险。

基于威胁的解决方案仅关注威胁方面，很多解决方案仅处理已知的威胁。基于风险的解决方案处理的是资产，将对资产的已知和未知威胁以及资产的漏洞都纳入到考虑范围。

在基于风险的安全模型中，安全保护的投资与风险成正比。

你应该根据所需保护资产的价值以及系统被入侵后可能导致的破坏程度进行安全保护投资。以家庭安防为例，对于一般的家庭，常规的门和门锁便足够了，但如果你经常在家里存放大量现金，就需要再购买一个保险箱；如果你还要在家里存放贵重的艺术品，那还要再投资一套家庭安防系统。越来越多的黑客受到的是利益驱使但没有政治目的。对于这些人，如果入侵所需投入的资源高于可能的回报，他们就可能不会再去实施攻击。.

企业可以根据基于风险的安全方法论在安全事件发生之前评估风险。对于贵重资产以及威胁和漏洞的重灾区，可以通过增加防御手段主动实施安全措施。如果新发现的威胁和漏洞导致风险级别发生变化，可以动态调整安全策略以确保重要资产的安全。

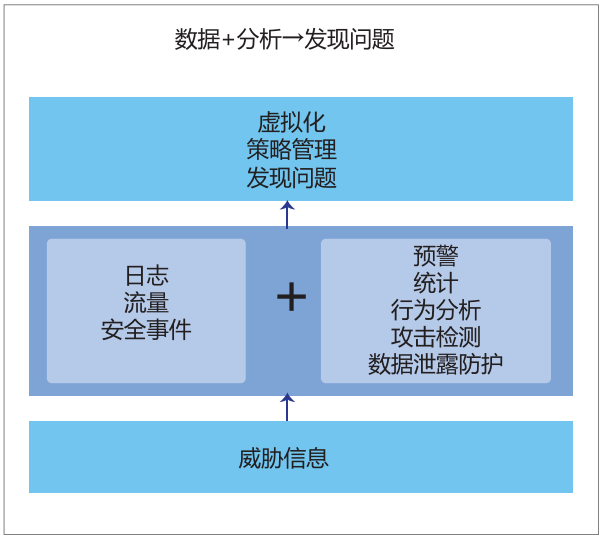
安全分析

传统意义上的网络安全产品以威胁为中心。为了应对所面临的威胁，我们引入了一些安全机制，而这些安全机制通常是基于特征的。在发现新的攻击后，要分析流量并将新流量特征添加到特征库中。系统监控流量匹配特征中的模式，如果找到匹配项，会将流量标记为可能的攻击。目前大多数的入侵检测和入侵防御系统使用的都是基于特征的引擎。

基于特征的方式非常适合于检测未加密的已知攻击，但也有非常明显的缺陷，也就是必须要知道攻击后才能够进行分析并编写新的特征。对于以多种形态出现的新的恶意软件和攻击类型、APT 及 0-day 攻击所带来的日渐增长的威胁，基于特征的方法基本上是无能为力的。

APT 和其他一些精心设计的攻击使用高度隐蔽的方式，几乎不留下任何可审计的线索，如日志和事件。一些可审计的日志和事

件由于数量过多，本身也不会提示严重的安全事件，但如果这些攻击是基于网络的，通常会在流量和流量数据中留下线索。大数据分析可以使用关联、机器学习等技术发现攻击的蛛丝马迹。

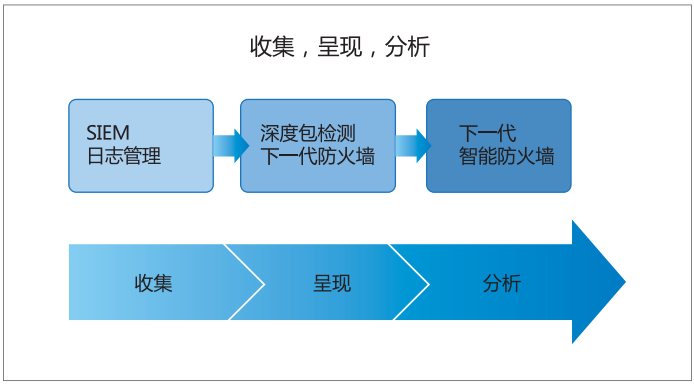


大数据分析技术分析大量不同类型的安全数据，可以轻松识别流量中的异常行为模式，对网络中用户和系统的风险评估是个重要贡献。如果必要的话，用户可以采取一些安全措施降低高危用户和系统暴露的风险，并增强对他们的监控。

网络计算和大数据技术的突飞猛进使得实时获取并分析大量系统日志、安全日志、会话信息、抓包文件等安全数据成为可能。流量数据和抓包文件提供了系统和事件日志中无法获取的宝贵信息。通过这些信息，数据分析系统可以:

- 分析用户行为，检测异常操作
- 分析应用行为，优化应用性能
- 分析流量模式，优化网络流量
- 检测数据泄露
- 检测网络中的僵尸网络

为实现上述目的，一些大公司使用了安全信息和事件管理(SIEM) 系统。SIEM 可以接受多个设备的数据并跨网络关联数据。这种方式的缺点是只能在事后进行分析，且无法对安全策略进行反馈和调整。

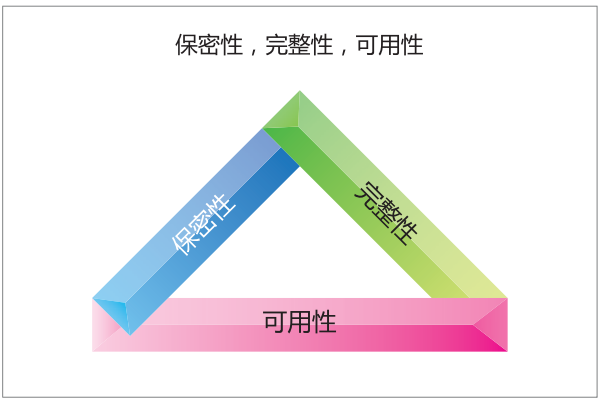


防火墙部署于网络中不同安全区域之间的关键位置，可以检测对安全策略和监控有重要意义的所有流量。防火墙演化到 NGFW 已开始收集流量和事件数据并将这些数据用于可视化，而最新的 DPI 技术可以将流量具体分析为应用和用户。有了这些信息，再加之以强大的硬件，防火墙可以近乎实时的分析数据，并根据网络中的变化动态调整安全策略。

防火墙中集成数据分析解决方案有以下一些优点：首先，可以提供最佳的响应能力。现代的 0-day 攻击从攻击开始到被检测之间存在时间差，而集成解决方案可以将这段时间缩短并减少破坏。其次，集成解决方案可以处理第三方解决方案不支持的各类实时数据。大量数据可以在本地进行处理，无需在设备间二次传输。现代分析依靠的流量数据比事件数据大几个数量级，这些数据的传输与否对解决方案的可行性有重要影响。最后但同样重要的一点，集成解决方案具有成本优势。这一点不仅体现在最初的采购阶段，由于无需管理多台设备，在日常运行阶段也可以节约成本。

安全和可用性

有一条被称之为 CIA 三元组的著名安全原则，指的是信息安全的三个组成部分。CIA 中的 C 代表保密性，被保护的数据不能被非授权访问；I 代表完整性，被保护的数据不能被非授权修改；A 代表可用性，要确保在需要的时候允许且可以执行授权访问。



业务应用和服务是当今企业的生命线。应用服务的可用性对日常运行和业务连续性至关重要，而业务中断或失败会在经济上导致严重的负面影响，在某些情况下甚至可能危及人命。云计算、移动技术和社交网络的发展趋势增加了 IT 基础设施的复杂性，其中网络本身作为一个基本单元也在经历快速的变革。传统上，企业使用网管软件监控网络状态，使用服务器管理系统监控应用状态。这两个系统的隔离可以为 IT 运行提供独立的视角，但也有缺陷，那就是无法显示网络和应用可用性之间的关系。这将导致更难事先预测应用问题，只能在事后进行排查。

- 拒绝服务 (DoS) 是针对安全模型的可用性方面的攻击，但系统中的可用性问题远不止 DoS 防护这么简单。
- DoS 和 DDoS 攻击：通过导致资源或系统不可用对系统进

行攻击。DoS 攻击分几种类型：带宽型 DoS 攻击使用大量流量占用可用的网络带宽；资源型 DoS 攻击使用有针对性的流量，每种流量都可以占用大量的资源，这样可以耗尽 CPU、TCP 连接等系统资源；崩溃型 DoS 攻击利用应用或操作系统中的软件 bug 导致应用或系统崩溃。DoS 攻击还可以分为常规 DoS 攻击和分布式 DoS(DDoS) 攻击：常规 DoS 攻击中只有一个攻击源，而 DDoS 攻击中有多个系统参与。

- 网络设备故障：设备或链路的硬件故障、设备软件 bug 等所导致的设备运行故障。
- 不适当的网络配置：路由环路所导致的通讯错误、不正确的交换机连接所导致的广播风暴等都属于这个类型，可能导致各种网络故障。
- 系统故障：由于服务器 / 存储硬件故障、软件 bug 等所导致的系统或应用故障。
- 不适当的系统配置：如果没有正确的配置系统或应用，可能导致应用服务故障或性能下降。
- 带宽分配和应用优化：即使所有的系统和网络都在正常运行，流量改变时也可能出现应用可用性问题。例如，如果 P2P 流量增加占用了所有带宽，视频会议和 VOIP 电话流量就可能受影响。
- 系统和网络运行中断。
- 人为因素，如不经意间断开链路。

可用性是一直被防火墙技术所忽视的因素。现在大多数防火墙中的防泛洪功能只能解决 DoS/DDoS 问题，且不能完全防范现代的 DoS/DDoS 攻击。

NGFW 存在的问题

NGFW 无法根据行为调整安全策略

下一代防火墙的基础是应用、用户和内容的识别，并根据识别结果实施安全控制。防火墙上配置的策略可以确定是否允许特定用户使用特定应用，安全策略基于应用、用户和传统的 IP 五元组（源 / 目的 IP，源 / 目的端口，IP 协议）。

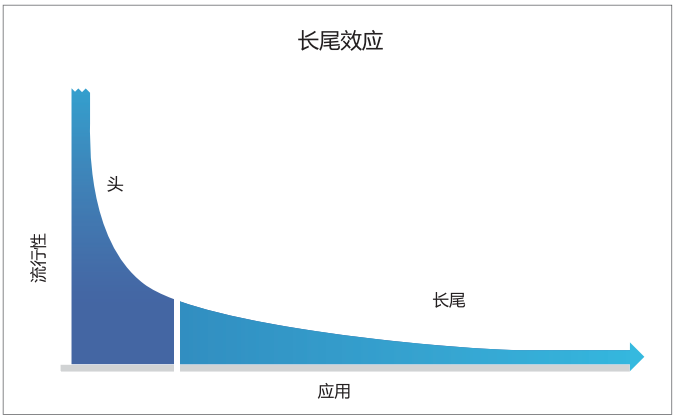
其他一些因素也可能影响用户的访问控制级别。在某个时间点使用应用可能是可以接受的，但在其他时间点使用就可能是可疑的，具体取决于用户或系统的使用历史信息。影响用户访问级别的一个因素是用户的风险级别，也被称为“信誉”。用户是否在执行可疑操作？如越级访问包含有恶意软件的网站。用户的机器是否显示出僵尸行为？如向外发起 DDoS 行为或联络已知僵尸网络的命令和控制 IP。用户是否在使用未打补丁的操作系统和应用？所有这些都可以成为限制用户访问关键资源的理由。用户的信誉可能随时间而变化，因此其访问级别也应随之变化。

NGFW 不会将用户行为关联到用户对流量的使用和其他事件上。具体来讲，NGFW 无法从时间维度上分析收集到的信息，因此只能对用户指定特定的访问级别，而无法进行动态的调整，但实际上用户可能需要根据感知到的风险改变访问策略。

NGFW 不会关注流量中的异常，包括与其他类似用户或系统所关联出的异常或随时间显现出的异常。例如，长时间没有太多行

为的用户突然变得活跃，或 web 服务器的响应时间和速度大幅度降低，这些都是应该调查的可疑事件。行为模式中的异常应对用户的信誉产生负面影响，访问策略也应随之调整。

应用的长尾效应



随着智能手机和 Web 2.0 使用的不断增长，应用的数量也大幅度增加。根据 2012 年 10 月份发布的消息，安卓和 iOS 平台上的应用数量均为 70 万个。Web 应用的数量实际上也体现出网站的数量。根据 Netcraft 在 2012 年 3 月所做的调查，当时大约有 6.44 亿个网站，且这个数字仍在以每月 5% 的速度在增长。我们尚未开始计算每个网站上应用功能的数量，但目前下一代防火墙可识别的应用数量仅仅有几百个到几千个。

这意味着有大量的应用没有被 NGFW 的应用识别所覆盖。如图上图所示，长尾效应表示某些应用不太流行，并没有被包含在防火墙的应用特征中，但由于数量众多，这些应用的总体使用量可能超过一些流行应用。

因此，部署策略可能无法实现预期的结果。如果用户希望阻断文件上传，传统防火墙可以识别并阻断基于 FTP 和 HTTP 的上传，NGFW 可以进一步增加更多的应用，如 box.com 或 Facebook 上传。但应如何处理属于长尾效应期间的文件上传程序和网站呢？可以正确的识别并阻断吗？

大量使用未知应用增加了系统的风险，管理员对此应有所警觉。对于使用这些应用的用户，应调整访问级别或实施额外的监控。

加密流量

应用识别还涉及到加密流量的问题。某些类型的加密传输 (如 SSL 和 SSH) 内容是可能被解密的，而对于不能解密的内容我们必须依靠流量行为模式进行应用识别。不能识别的流量只能被整体的全部允许或拒绝。我们可以将已知的应用添加到白名单，并拒绝所有未识别的流量。但实际上，由于上文所述的应用长尾效应，总有些应用属于未识别的类型但被无意中阻断，导致需要 IT 支持，用户体验也会变差。

大量使用有加密的应用还可能影响系统的风险级别，管理员应考虑对这些用户应用不同的访问级别或监控策略。

下一代智能防火墙

iNGFW 对安全和流量数据进行深度的数据分析，并进行主动检测，这样可以为用户提供基于风险的安全保障。管理员可以基

于感知到的风险进行安全管控，在事发之前防范安全问题或系统网络中断。iNGFW 的增强型 NGFW 功能允许用户全局总览网络、用户和应用，并动态控制策略。

iNGFW 可实现以下功能：

- 主动检测网络，iNGFW 使用大数据分析技术检测异常行为和系统资源使用情况，防范 0-day 攻击。行为信誉指数 (BRI) 是对内网用户、主机和服务的信誉衡量，可以呈现与内网资产相关的风险。
- 主动检测资源、网络和服务的可用性，降低服务中断的概率，减少中断时间；对用户、资源、网络、应用使用情况和行为进行风险分析。全网健康指数 (NHI) 可以评估系统所面临的安全和可用性问题，呈现整个网络和每个子网的健康状况。
- 通过 BRI 和 NHI 报告系统风险。如果目标对象或网络的健康状态发生变化，系统会生成告警。
- 根据目标对象的 BRI 和 / 或子网的 NHI 动态调整访问控制和流量控制策略。策略控制基于八元组：信誉，IP 五元组，应用 ID 和用户 ID。
- 智能 QoS 实现细粒度控制用户和应用流量，保障关键业务应用的可用性。
- 用户、资源、网络和应用使用情况及相关风险评估结果可视化。

行为分析和行为信誉指数 (BRI)

iNGFW 实时监控流经设备的流量并收集流量信息，其间统一威胁检测引擎结合最新的威胁情报生成安全事件日志。iNGFW 数据分析系统实时的处理这些数据，分析与内网用户、主机和服务相关的风险。内网对象的风险级别是通过行为信誉指数 (BRI) 呈现的，这个风险级别也可以动态影响对内网对象所实施的策略。

在分析阶段，iNGFW 首先使用应用和用户识别技术对收集到的数据进行分类，目标对象可以是用户、主机或服务。目标对象的行为指的是特定时点与网络中信息和资源使用情况相关的信息集:

- 流量使用情况:
  - 流量信息
  - 带宽
  - 应用组成
  - 请求速率
  - 响应时间
  - 访问该对象的源
  - 该对象所访问的目的
- 源自对象的攻击
- 针对对象的攻击
- 系统信息
  - 设备信息
  - 操作系统版本
  - 补丁信息
  - 应用程序信息 (杀毒软件、下载程序等)

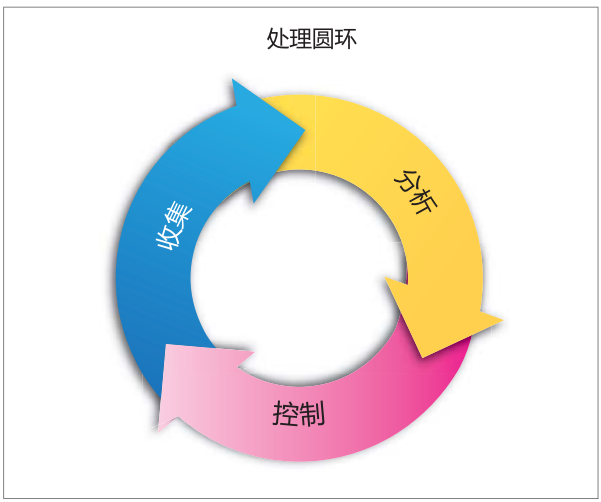
iNGFW 对内网对象引入了行为信誉指数 (BRI)，用于说明对象的健康状况和风险级别。

对象的信誉可能取决于多个因素:

- 对象的当前行为。
- 对象的历史行为: 可以是攻击事件史、应用使用情况史等。
- 与同类对象的行为对比: 如果用户的使用模式与其他用户差异明显，应对该用户重点关注。
- 对象行为的历史变化情况。

之后 iNGFW 使用数据分析技术和机器学习技术查找显示出有问题的行为和模式。

- 网络和系统使用情况是否符合公司的相关规定。大量使用社交和媒体应用可能说明工作效率问题，大量未知应用的使用可能是需要进行关注的安全违规事件。
- 与历史数据比较得出的正常网络和系统使用情况。行为突变不一定说明出现了问题，但对有些情况需要提高警惕：Web 和应用服务器上突然出现新的服务，长期休眠的用户突然出现大量活动。
- 与同类对象比较得出的异常网络和系统使用情况。应对大量使用与业务无关应用的用户进行调查，如使用 P2P 或未知应用的用户。
- 关联事件日志和流量特征进行僵尸网络检测。



数据分析系统的一个优势是能够检测数据泄露。这类数据泄露通常伴随有异常应用使用或异常行为，异常行为中通常会出现用户访问过多的服务器以及大量的拒绝访问。用户可能使用大量的可疑应用，如下载程序、代理、隧道或未知应用。

高级持续威胁 (APT) 是一种更加精心设计、更有组织、更有针对性的攻击。APT 攻击的行为更具伪装性，依赖于单个事件的检测会产生过多的误报，并无实用价值。行为检测系统能够分析大量不同类型数据，通过关联事件找出此类攻击的蛛丝马迹。

深度数据分析也可以发现网络中受感染系统的行为。受感染的系统会寻找到命令与控制 (C&C) 服务器和外发攻击的连接，早期检测到这些系统可以警告管理员系统已被入侵，并有助于限制系统入侵所导致的破坏。

iNGFW 提供的基于风险的安全管理可以展现系统中内网对象的信誉。行为信誉指数 (BRI) 基于行为分析衡量对象风险。通过集中关注具有最高风险的目标及与这些目标相关的行为，管理员就可以专心处理系统中最严重的问题。

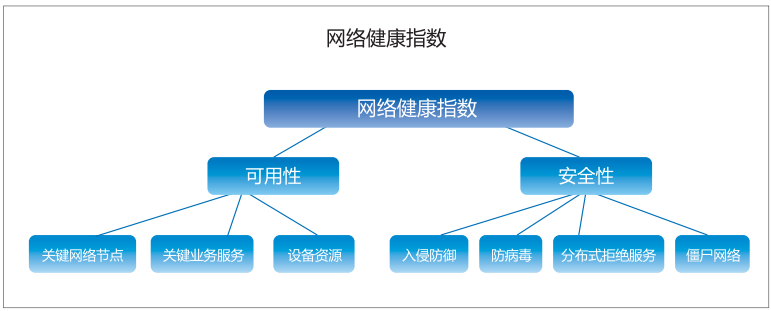
在 iNGFW 中，安全分析可以通过基于信誉的访问控制动态的融入到安全策略中。二者的结合可以缩短问题出现与修复之间的时间。

主动检测和全网健康指数 (NHI)

iNGFW 保护应用可用性和保持业务连续性的一个方法是主动监控。iNGFW 通过定期探测监控网络中的应用、服务器和关键节点和资源消耗，并关联分析探测结果以总体评估网络的健康情况和服务的可用性。在运行状况开始恶化时，管理员会在服务完全不可用之前获得预警。出现问题后，系统还会提供每个检测单元的完整健康报告。这有助于用户进行故障排查并缩短确定故障所需的时间。

可监控的指标包括:

- 网络链路上的流量
- 流量中的应用组成
- 网络设备的丢包率和延迟
- 服务器的丢包率和延迟
- 应用和服务的失败请求和延迟
- CPU、内存、会话等系统资源



全网健康指数 (NHI) 用于衡量影响网络中网络和服务可用性的风险。系统会通过连接的针对接口或安全域计算每个子网的 NHI。健康状态发生变化时，系统会通知管理员采取预防性措施。

健康状态分三种:

- 健康：网络和服务运行正常。
- 亚健康：尽管服务没有中断，仍存在可能导致严重问题的情况，如持续的高 CPU 使用率或资源接近耗尽。管理员应缓解问题以防范故障。
- 危险：出现了严重影响网络和服务正常运行的问题。

全网健康指数用于评估网络、系统和应用的业务交付能力，可分为两个单元：安全评估单元和应用及服务可用性单元。

安全评估单元通过系统中的安全事件和漏洞确定系统的已有

或潜在威胁。对于构成风险的三个要素，该单元会对其评估系统威胁和漏洞。

- 威胁状态：包括攻击与被攻击所产生的威胁。
- 异常行为分析：在安全数据中分析异常行为。异常可能是与同类对象做比较得出的，也可能是与历史数据做比较得出的。
- 漏洞检测：扫描网络中系统的漏洞。终端代理也可以报告有关设备的合规性信息。

应用及服务可用性单元由三个监控组件支撑：服务器和应用监控，网络设备监控和资源监控。

- 服务器和应用监控：监控服务器和应用的响应时间。
- 网络设备监控：监控网络设备的连通性和延迟。
- 资源监控：监控 CPU 使用率、内存使用率、会话等关键系统资源。

监控单元或组件的健康指数大体上是通过计算其全部子组件的健康指数得出的。每个单元、组件和子组件都有亚健康和危险状态阀值。总体来讲，如果任何子组件处于危险或亚健康状态，则其中包含的组件和整个系统都会处于危险或亚健康状态，这样可以确保本地问题可以传递到顶层并呈现给整个系统。

通过每个监控单元、组件和子组件的健康指数，我们就可以计算整个网络的健康状况。监控组件的多级架构有助于管理员主动锁定和诊断问题点。

除了资源监控，还可以对防火墙的接口或安全域进行监控和安全评估。基于接口或安全域将网络划分为多个子网后，就可以计算出每个子网的 NHI。例如，如果在 DMZ 安全域中检测出僵尸，DMZ 的风险级别会提高，但没必要提高网络中其他部分的风险级

别。NHI 允许用户方便的查看每个网络的风险级别，同时总体评估整个网络的健康状况。

基于信誉的访问控制

内网对象和子网可以根据行为信誉指数和全网健康指数分为三种健康状态：健康、亚健康和危险。iNGFW 使用基于信誉的访问控制，基于八元组应用访问控制和流量控制策略：健康状态，IP 五元组，应用 ID 和用户 ID。

企业可以利用基于信誉的访问控制为处于不同健康状态的用户设计不同的策略。对于处于危险状态的用户，应进行隔离并分配到需要修复的网络中，或仅提供类似于网络访客级别的访问；对于处于亚健康状态的用户，应禁止访问网络中敏感的或高度保密的资源。如果由于健康状态导致访问受到限制，应通过终端代理或网页弹出框通知用户，这种举措有助于用户联络网管主动修复问题。

类似的，全网健康指数也可以影响不同接口或安全域之间的策略。可以根据接口或安全域相关子网的健康状态动态更改策略。

由于随时可能会发现新的攻击或漏洞，设备故障也可能影响可用性，因此 BRI 和 NHI 都是随时都会变化的动态数字。当 BRI 或 NHI 变动到足以影响目标对象或网络的健康状态时，可以动态调整访问级别以降低风险。

BRI 和 NHI 有助于管理员锁定高危区域并主动修复已有和潜在的问题。基于信誉的访问控制允许管理员通过限制暴露敏感信息降低风险。

总结

高级威胁和 0-day 攻击的本质是高度可规避检测，导致基于特征的防护越来越无计可施。安全保护模式正在从基于威胁的保护向基于风险的保护转变。iNGFW 是基于风险的安全解决方案，优于增强型下一代防火墙。通过持续监控、收集和分析流量及可用性数据，iNGFW 主动查找可能影响网络运行的异常行为和潜在的网络问题。iNGFW 提供了两个指数：全网健康指数是网络和服务中潜在安全和可用性风险的概括性指数，行为信誉指数是对每个内网对象（用户、服务器和服务）的健康状态和风险级别的衡量。基于信誉的访问控制将健康状态和风险级别与访问级别关联起来。通过基于感知到的风险动态调整访问级别，iNGFW 可以帮助管理员降低企业网络和服务的运营风险。

关于 Hillstone Networks

Hillstone Networks 成立于 2006 年，专注于网络安全领域的前沿技术创新，为企业级和运营商用户提供智能化、高性能、高可靠、简单易用的网络安全解决方案。Hillstone 以网络安全的需求变化为创新基点，立志为全球用户打造安全的网络环境，成为世界第一流的受人尊敬的安全厂商。从最初的五人创始团队发展至今，Hillstone 已拥有员工 600 人，在北京、苏州、美国分别成立了研发中心，建立了 20 多个销售分支机构，成为网络安全领域的领导企业。

Hillstone 的旗舰产品下一代智能防火墙在业界首次用智能的关联分析方法实现基于信誉的安全管理控制，帮助用户在应对各种安全威胁的基础上，提升企业防范风险的能力，最大程度保障企业业务可用性。Hillstone 的数据中心防火墙产品，以分离式的硬件架构结合分布式的全并行处理，将性能和容量的弹性扩展提升到一个新的高度。Hillstone 的安全产品基于其独创的 64 位全并行实时安全操作系统 StoneOS®。Hillstone 拥有几十项国内外发明专利。

据国际权威市场研究机构 IDC 发布的“2012 年度中国 IT 安全硬件市场分析报告”显示，Hillstone 以 13.9% 的市场份额占据中国 UTM 硬件市场第二，在世界 500 强公司和重要行业客户中得到了广泛的应用和部署。2012 年，Hillstone 被创投界的“硅谷圣经”——《Red Herring》杂志授予“2012 全球创新百强企业”，全球知名咨询公司 Frost & Sullivan 授予 Hillstone“2012 中国区统一威胁管理市场增长领导奖”。

Open the book and find:

- What is the limitations of threat based security approach?
- Do you have the capability to visualize risks faced by networks and users?
- How is iNGFW different from existing UTMs and NGFWs?