Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 1, Issue 1, 2015, pp 15-18
ISSN: 2395-0196

A STUDY OF ISA SERVER FOR PROVIDING FAST INTERNET ACCESS WITH A SINGLE PROXY

MANISH JHA[1]
[1]*Assistant Professor, Maharishi Arvind Institute of Engineering and Technology, Jaipur*
**Corresponding Author, Email : manishjha879@gmail.com*

Abstract: The Microsoft is an Internet Security and Acceleration (ISA) Server 2006 is an integrated firewall, VPN remote access (VPN), VPN site-to-site, Web Proxy, and a solution of server caching. ISA Server 2006 can be configured for act in these roles or every subset of them. This allows ISA Server to provide a flexible network security appliance for enterprises of all sizes. The security model of ISA Server 2006 is built around the nucleus of firewall. The basic features of the firewall ISA Server 2006 supply an anchor point for all ISA Server roles as a security network. The discussions in this paper are limited for the basic firewall ISA Server 2006. Further components such as ISA Server Web proxy filter, specific applications filters or extensions VPN ISA Server 2006 are not discussed unless as regards core services firewall ISA Server 2006.

Keywords : VPN, ISA, Firewall, Networks

INTRODUCTION

The nucleus of ISA Server firewall depends on the following elements and their interactions:

- Specifying the network interface driver (NDIS) and Microsoft Windows Networking Stack ;
- The Firewall Packet Engine;
- Microsoft Firewall service.

Figure 1 shows a conceptual view of the kernel and user-mode components of ISA Server 2006 and displays the relationships between components.

The Firewall Engine and Windows network components are in kernel mode, and engine components of policy are accessible scheduled in kernel mode firewall engine. The rest of the architecture ISA Server 2006 runs in user mode.[1]

NDIS AND THE WINDOWS NETWORKING STACK

At the lower layers in ISA server2006, one can see the NDIS stack and TCP / IP protocol. Both of these components of Windows operating system execute in kernel mode, the Enhancements of the Windows networking stack and enables the developers to force into network stack at very low level access for packets filtering and other services before they are fully deal with the operating system. ISA Server 2006 takes full advantage the application programming interfaces to enhance packet filtering and application and the performance firewall layer.

Two specific hooks used by ISA Server 2006 include the hook filter and firewall hook package. They are located at the bottom and top of the Windows networking stack, respectively. Although NDIS stack and TCP / IP protocols are parts of the operating system, remaining blocks in the diagram represent the ISA Server 2006 components.

FIREWALL ENGINE

The firewall engine is also called the firewall packet engine and the service of the firewall are two core components firewall ISA Server 2006. These components used in the Windows networks hooks programming the battery described above. At the foot of the protocol stack, kernel mode firewall engine receives all the packets through the firewall TCP / IP hook. The packets are associated with a connection rule then all the packets are inspected. If packets are allowed at this stage (low layer), then the firewall policy is applied. The manipulation of these operations in kernel mode enhances the performance and security of the network . If the Firewall service has already authorized all the packets, then

firewall engine can create a data pump in kernel mode. This examines the type of processing in relation File Transfer Protocol (FTP) operations. After firewall engine has finished operations, packets are still moving through the Windows networking stack, where the normal processing such as reassembly of packets and routing occurs.[2]

FIREWALL SERVICE

The service firewall works in user mode, on top of the the protocol stack TCP / IP, and uses a hybrid architectural combination elements from both proxy and behavior of state ful firewall inspection. The service firewall performs an inspection of the additional packets after the authorization by your firewall engine. The Firewall service has the ability to handle the traffic across multiple connections and perform a processing partner, such as filtering application.

Application filter API

API application filter is set on top of Firewall service. This API supplies extensibility for developers to integrate additional filters implementing on specific application layer protocols. This enables ISA Server 2006 to fit new applications and application protocols which appear on the market and as a result updates and improvement of Windows operating system.

Web Filter API

Located on top of filter Web Proxy API Web Filter. This API is an API higher than the level of implementing folder. While the API application filter is mainly focused on the transmission control protocol (TCP) and User Datagram Protocol (UDP) sessions the connections and sockets, API Web Filter specifically manages Hypertext Transfer Protocol (HTTP) and secure HTTP (HTTPS) provides communications and processing notifications and other targeted protocol tasks on the Web protocol.

Policy Engine in the ISA Server

The policy engine communicates with all the components of the base of ISA Server firewall both along with the kernel firewall engine mode and service the firewall in user mode. In addition, the policy engine communicates with the two layers of filters and implementing on the Web. An advantage of this device is enhancing performance and stability, because the policy is processed in kernel mode.[1] Information of the basic elements of the firewall ISA Server 2006 This section presents the Detail components the firewall ISA Server 2006 database. As seen above, the basic elements of the firewall are kernel driver firewall Packet Engine and service firewall user mode. The driver for the firewall engine is set to inspecting the network traffic sent and received by the firewall. It can move on the traffic decline in traffic, or transmit the request to the service the firewall. If it is passed at the service of firewall service the firewall shall determine whether to pass or drop traffic.[3] The firewall services consist of following components which also perform the various tasks in their respective areas :-

- Firewall traffic control, which includes:
  - Rules engine
  - User-mode data pump
  - Server publishing
  - Firewall client listener
  - Connection limits
- Firewall support services, which includes:
  - Domain Name System (DNS) cache
  - Connectivity monitoring
  - Lockdown monitor
  - Network configuration detector
  - Dial on demand
  - VPN interface
- Firewall management, which includes:
  - Logging
  - Statistics provider
- System infrastructure, which includes:
  - Buffer management
  - Sockets and socket pools
  - Thread pool

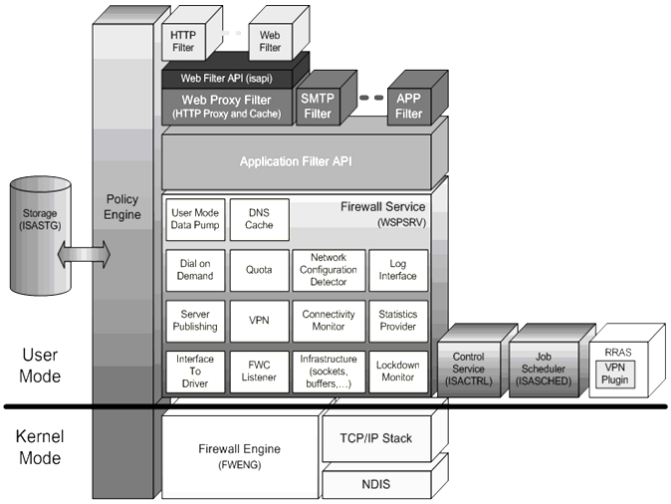

Figure 1. Firewall Core Structure

A. Firewall Packet Engine in the ISA server

It is a kernel -mode driver. The driver for the firewall engine is invoked each time the network traffic arrives or leaves an ISA Server network interface and modify if necessary. No network traffic is sent whether the driver of the firewall engine does not permit it. The hooks of engine driver firewall in Windows protocol stack network in two places. The first place is at an early stage in processing packets after IPsec (Internet Protocol) driver, but before any reassembling takes place. This may be considered as a filtering layer from layer 2 (the Media Access Control) layer and 3 (network).[1]

At this stage, the driver performs the several tasks.

- Intrusion detection.
- Spoof detection.
- IP options policy checking.
- Logging dropped packets (if configured to do so).

The driver for the firewall engine attempts to associate all the packets it receives with a connection policy, based on the source IP address, protocol and port, and destination IP address, the protocol and port. There are the following features for connection rule policy.

- Protocol number
- Source (IP address, and port or start point)
- Destination (IP address, and port or endpoint)
- Source address translation (optional)
- Destination address translation (optional)
- Statistics (number of bytes transferred and last access time)

FIREWALL SERVICE

There are the following services of the firewall policy.

- Performs policy decisions that cannot be made by the Firewall Engine driver.
- Handles all Firewall Client traffic.
- Handles server publishing rules.
- Performs logging (for itself as well as on behalf of the driver).
- Acts as a Web proxy.
- Hosts application filters.

FIREWALL CHAINING IN THE ISA SERVER

In this scenario, a firewall (firewall downstream of said) acts as a client of the firewall that a firewall is another firewall (firewall called upstream). The firewall determines downstream request to send firewall upstream using a similar algorithm to Client Firewall itself. It inspects requests, and if they are targeted an address which is not in the local network it received from upstream. As composing on demand when a firewall chaining is defined in kernel mode for packet routing is disabled, resulting in lower performance.

Another major issue in the the firewall chaining is that a firewall downstream requires a successful recovery of the the local address table (as defined by the configuration of the network element on which the listener Client Firewall is created) and the local Domain Table (as defined by the configuration of the network element on which the listener is created firewall client) firewall upstream to run correctly. After the extraction was made, the information that the firewall is back upstream is used until the next successful recovery. If traffic is sent through the firewall before it has a chance to get the information the firewall upstream will be blocked. Another important issue the firewall chaining is a scenario where the downstream ISA Server computer to is by chaining a firewall on the computer upstream ISA server. After the establishment of the connection on TCP port 1745, Winsock uses a wide range of customer ports to connect to the computer upstream ISA server. Because normally the ports are not open on a firewall between the ISA Server computer, you must either to open all ports or change the architecture. The solution is to allow all traffic between the upstream and downstream ends.

SUMMARY

ISA Server 2006 is a comprehensive firewall, remote access VPN, VPN from site to-site and Web proxy and server solution that caching. ISA Server 2006 can be configured for operate in these roles or any subset of them. This enables ISA Server to provide a flexible network security solution for businesses of all sizes and with different security requir-ements. The kernel and the firewall ISA Server consists firewall engine driver and the firewall service driver. The driver firewall Engine runs in kernel mode and the service the firewall running in user mode. The driver firewall engine is in the protocol stack. Windows network at a low to intercept packets before they reach the protocol stack in, Windows TCP /IP and re-injects these packets in the stack level after state ful inspection and applying all the policy of firewall. The service the firewall receive packets from the driver the firewall engine for more advanced treatment. The service includes a firewall interface API application filter, which allows the service the firewall to perform an inspection based on the rules for the application layer protocols. In addition, the firewall service offers a range of services, including DNS caching, logging, auditors, and much more support.

Advantage of ISA server.

1. The forms is generated in the firewall is a form based authentication;
2. It is easy –to- use wizards;
3. It is easy- of use management features;
4. It is the real time monitoring of log entries;
5. It is a multi layer firewall;
6. It provides security in the network;
7. Lower cost in deployment;
8. If any undetermined the Active Directory, they can possessing the ISA Firewall;
9. If Firewall is owned, Active Directory can be Accessible.

Disadvantage of ISA server.

1. Limited bandwidth;
2. The server certificate must be require on the CSS while working in ISA;
3. It is necessary to track the certificate; status for the avoidance of expired certificate;
4. No support for the outgoing access user / group control based unless for Web traffic;
5. Without the user certificate authentication no any one can use it.

Validation of ISA server against the credentials:

1. Active directory;
2. Active directory via LDAP;
3. RADIUS;
4. RSA secure ID.

REFERENCES

[1] Martin Eisermann, "Performance tests with the Microsoft Internet Security and Acceleration (ISA) Server", 2002.

[2] TNT soft, "Real Time Monitoring for Microsoft ISA Server:, 2002.

[3] Leeven Chang, "ISA Server", 2005.