The concept of isa server

An Internet Security Acceleration (ISA) 2006 Server acts as both an enterprise firewall and a web proxy/cache server. It has the capability to screen all packets, circuits and traffic passing through most applications either within or outside the network. The web cache inside ISA Server 2006 can store web content in a bid to reduce traffic on the network and provide faster access to web pages and other web applications that are frequently accessed by users on the network.

ISA Server 2006 also has the capability to schedule the download of web page updates for specific times of the day that record less traffic to ensure an optimal and less frustrating use of the internet. ISA Server 2006 has in-built features that allow administrators come up with policies for regulating usage of network resources based on criteria such as applications, groups, destinations, schedules and content type criteria. It can also work with Windows 2000 and older operating systems.

The Windows Kerberos Security is an additional facility that can be utilized with ISA and it comes with a software development kit (SDK). ISA Server 2006 is available in two editions: the standard edition and the enterprise edition. The standard edition supports up to four processors at a time while the enterprise edition is more suitable for large scale deployments, multi-level policy implementations, server array support and computers that have more than four processors. ISA server licenses are usually given out based on the number of users present in the organization.

ISA Server 2006 may be further described as a firewall security product that was designed to publish web server and other server systems through the use of firewalls, VPN endpoint, and can also be used to provide internet

access to clients in a networkingenvironment. ISA Server 2006, according to the Microsoft definition, is the integrated edge security gateway that helps to protect any environment that deploys informationtechnologyinfrastructure. It shields the environment from threats from external networks, especially the internet, and also provides users with access to applications and data in a secure fashion. Turner construction mission statement

ISA Server 2006 gives further value to the work of IT Managers, network administrators and information security professionals who want to manage security and reduce the cost of performance of network operations (Microsoft, 2009). Core functions of ISA Server 2006 ISA Server 2006 has the ability to streamline the provision of security for applications accessed over the internet. They can be used to connect corporate networks in a robust and secure manner; this helps to reduce network costs by leveraging on existing network infrastructure (Microsoft, 2009).

They can also be used as a wall of defense against attacks to the network. Organizations are faced with so many advanced and sophisticated attacks on their computer systems and it is becoming increasingly important to protect all corporate resources and simultaneously provide business functions. ISA Server can be effectively deployed in small to medium-sized organizations with varying number of sites and networking needs. ISA can also protect clients and ensure that an organization’s resources are available to all employees even in far locations of the world (Microsoft, 2009).

Features of ISA Server 2006 ISA Servers provides three types of firewall configurations and these can be operated in different modes. These modes are packet filtering, stateful filtering, and application layer filtering. It has

features for compressing and caching data that makes it easy to accomplish remote connection across branch offices (Berghel, 2002). The in-built HTTP Policy of ISA Server also makes it easy to prevent connection attempts to the Microsoft Windows Operating system, regardless of the file extension used in attempting this.

It can also reduce bandwidth utilization through web caching (Portcullis Systems, 2009). New concepts of ISA Server 2006 ISA Server 2006 came on board with new concepts and some of these new features are discussed here. Arrays Arrays refer to a collection of computers that are located together within an area, for example, around a department or office. They can be domain arrays that use active directory or they can be independent arrays that allow the storage of information in a local configuration database (Serwin, 2004). Rules

Rules are what the system administrators use to set up specific protocols to govern contents, sites and IP packet filters that pass through a network. An array policy can be applied to a specific array. Enterprise policies contain the same type of rules applied to array policies but they are usually applied to many arrays at the same time (Serwin, 2004). Firewall The firewall is used to enhance stateful packet inspection and constitutes a medium of ensuring enhanced security by analyzing data packets at the protocol level and the connectivity level.

Policy-based administration is another component of the server firewall. The ISA server allows administrators to manage and develop policy rules. Policies are a set of rules through which users, protocols and groups of users operate. A specific type of policy can apply to a single array or the entire

enterprise (Serwin, 2004). Virtual Private Network Support ISA is an easy way of creating VPN-based networks. There are numerous wizards in the ISA application that can help to install security options (Bell, 1993). Intrusion Detection System Support

ISA Server comes with an intrusion detection system. It has in-built features that help to prevent attacks such as Ping of Death, UDP bombs, POP Buffer Overflow, Scan attack and so on. Other notable components of the ISA Server include the Web Cache Reverse and Scheduled caching programs that can help to improve the performance of the system reporting features. ISA has many report-generating features that allow for improved management of the ISA Server. Gatekeeper H. 323 component of the ISA Server allows the supervision and management of IP telephony calls.

ISA Server 2006 delivers secure access to client machines on the network without any need to configure clients separately (Serwin, 2004). Risks faced by IT Networks There are numerous threats that networks in most organizations face today. Some of them may come in the form of Denial of Service attacks, worms, viruses, information compromise and so on. For any company that intends to do business online, it is important to combat these increasing threats which have the capacity to multiply on a daily basis (Portcullis Systems, 2009). Misconceptions about ISA

Computer systems are being constantly exploited all over the world. ISA Server 2006 is becoming increasingly relevant to organizations that are beginning to see that the traditional firewalls and related technologies aren't able to combat the attacks they are subjected to effectively. Most of the controversy associated with ISA stems from the misconception that most

people have about the role of ISAs. Some people think that ISA is only a proxy server. This is incorrect. It can act as a firewall, VPN, web-caching proxy and application reverse-proxy solution.

Features such as intrusion detection, content filtering and application filters all help to extend the capabilities of the ISA Server in fulfilling the dynamic needs of the IT environment (Berghel, 2002). To clear up the rampant misconceptions about ISA Server 2006 and its capabilities, it’s important to make an intelligent comparison between it and other prominent solutions in the market today. ISA Server is unique and different because it comprises features such as Virtual Private Network (VPN), application layer firewall, web cache services and numerous security features all rolled into a single package.

There is no other product that contains such a robust combination of security solutions in one package. The solution also integrates back-end infrastructure such as Windows/IIS Exchange Server, Windows SharePoint services and other compatible products (Microsoft, 2009). There are many features that make the solution very attractive to most organizations and some of them include the presence of wizards for publishing server resources, authentication through forms, and customizable security solutions for Exchange and Windows SharePoint services.

In conclusion, ISA Server provides an interface for Windows servers, clients, application infrastructure and other data resources to connect unlike other firewalls. ISA Server has been customized to protect Microsoft applications. Applications like Microsoft Outlook Web Access can be optimally utilized by using its features such as remote access. ISA Server 2006 is easy to manage

and deploy at target locations and can help to achieve huge cost savings in time, moneyand resources. It can be customized to work with other security applications such as intrusion detection software, antivirus solutions and the different types of firewall.

It can also complement existing solutions by providing an additional application-level protection against network attacks (Microsoft, 2009). A variant of IAS Server 2006 is the hardware-based solution. Microsoft recently joined the league of OEMs to bring security appliances and gadgets into the market. The solution comprises a version of Windows Server 2003 and hardware optimized for effective use. This customized hardware is best used when the ISA Server is needed specifically for running ISA Server 2006.

Misconceptions about ISA are that it functions only as a firewall and was introduced to replace other firewall solutions within the network. ISA Server 2006 is much more robust than most organizations think. The usual notion in most organizations is that hardware firewalls are more secure. This is not altogether true. Application layer firewalls like ISA 2006 can be easily customized, are powerful and cost-effective for organizations of varying sizes. ISA for example, can be used to connect remote locations to one another without the need of deploying expensive hardware like routers and the like.

ISA security is not restricted to only when a person is connecting to the internet from the inside but also works effectively when a user is connecting to the internal network through the virtual private network. In addition to being a fully functional firewall solution, ISA Server contains a host of other security and productivity features (Microsoft, 2009). History of Hardware and

Software firewalls Introduction to Firewalls Firewalls can be described as layers of security in a network that protect the network from threats and other malicious attacks from outside.

There are two main types of firewall and these are the hardware firewall and the software firewall. The hardware firewall is an impenetrable unit of hardware that has a port through which configurations can be made to allow access into the network or prevent access into the network, depending on the nature of the traffic. An example of a hardware firewall is the Cisco PIX Firewall which is configured with the use of access lists and Cisco IOS. Software firewalls on the other hand, are installed on the systems that need protection.

They can perform the same function as the hardware firewalls but can easily be compromised. Examples are Windows Defender and Vista Firewall. They are able to monitor the programs installed on any particular machine and the user can select what program should run or not. A firewall can be described as a software program that is used to control and monitor the transmissions, data influx and information exchange between the computers in an organization’s internal network and the internet. Firewalls are usually installed at the edge or entrance to the network to prevent inappropriate access to the resources of the network.

The firewall ensures that only legitimate and harmless data is exchanged and that the security policies of the organization are strictly adhered to. A firewall can be implemented both as hardware and as software. It can also exist as a combination of the two. Firewalls can help to prevent hackers from entering a system and gaining access to confidential information. They are

more restrictive to users from the outside than those from the inside. Some firewalls also contain features that allow auditing, logging and trailing of user actions.

It provides information to the administrator on what type and volume of traffic has passed through the network at any particular time. Michael Gregg, an expert in security observes that the National Institute of Standards and Technology (NIST) categorize firewalls into the following categories: Dynamic, Kernel, Packet filters, Stateful Inspection, and proxies (Al-Tawil ; Al-Kaltham, 1999). These categories are however, not established because most firewalls possess attributes that are characteristic of one or more of the following groups outlined above.

Another broader classification by expert Chris Partsenidis breaks down the types of firewalls into two broad categories. These are Network layer firewalls and application layer firewalls. Network layer firewalls operate by examining the source address, destination address and the port numbers through which traffic or data packets pass. A router is an example of a network layer firewall. Modern network layer firewalls can maintain information about the state of the connections that pass through them at each particular point in time.

They are able to accept traffic through them. This means that data packets that flow through these routers must have been assigned a valid IP address block or a private internet address block. These types of firewalls are fast and transparent to their users during their deployment and utilization. Application layer firewalls may be described as host systems that have proxy servers installed on them. They do not permit the direct exchange of traffic

between networks; they perform logging of events and general traffic monitoring.

Since they come in the form of software, they can be used effectively for developing access control lists and logging. They can also be used as network address translators. They provide network security with a more granular approach. The Development of Firewalls In the past, users were not always aware of the presence of application layer firewalls and therefore required some training. Today, modern application layer firewalls are transparent. Application layer firewalls are usually a more conservative security model to deploy and are better for organizations that require detailed audit reports.

The current trend is the production of firewalls that have characteristics of both network layer and application layer firewalls. New products are more likely to be centered on packet screening, logging of details and checking data that pass through them. Proxy firewalls are another classification of firewalls that offers comprehensive security to networks. Organizations that deploy them however have to sacrifice some speed and functionality because they impose restrictions on the applications that can be supported by the network.

Unlike some other types of firewall that just block access to certain data packets flowing through the network, traffic does not flow through a proxy. The proxy serves more as an intermediary device that initiates a new connection on behalf of any request that flows through the network. This method prevents directcommunicationbetween two systems on both sides of the firewall and makes it harder for the malicious attackers to identify where

exactly a particular network is located because data packets are not received directly by the target system.

Proxy firewalls can also offer protocol analysis security. They have the capability of looking at the data packets and the network protocol used for communicating. This makes them more effective than other security solutions that merely focus on the packet header information. Another category of firewalls known as unified threat management (UTM) has emerged. This category has various security promises and is useful for all kinds and sizes of businesses.

UTMs are usually capable of performing intrusion detection, content filtering and spam filtering altogether. They can combat different levels of malicious threats all over the network and are usually designed to offer protection from next-generation application layer threats. They can also conduct central management through a visual console without affecting the overall network performance. UTMs are convenient, easily deployed and cost-effective. Some of the leading UTMs in the market include NetScreen, Symantec, WatchGuard Technologies amongst others