5.3.5 Security Solution Facts

The following table lists additional network security solutions that can be configured to increase network security:

Device	Description
Proxy Server	A *proxy server* is a type of firewall that stands as an intermediary between clients requesting resources from other servers. A proxy server is often called an application-level gateway because it performs filtering at the application layer. Proxies can be configured to: - Restrict users on the inside of a network from getting out to the internet. - Restrict access by user or by specific website. - Restrict users from using certain protocols. - Use access controls to control inbound or outbound traffic. - Shield or hide a private network to provide online anonymity and make it more difficult to track web surfing behavior. - Cache heavily accessed web content to improve performance. Proxy servers can also be a security risk and can be used to circumvent network security and even attack a network.
Internet Content Filter	An internet *content filter* is software used to monitor and restrict content delivered across the web to an end user. Companies, schools, libraries, and families commonly use content filters to restrict internet access, block specific websites, or block specific content. - Two types of configurations are commonly used: - Allow all content except for the content you have identified as restricted. - Block all content except for the content you have identified as permitted. - Allowed or blocked content is identified by the following: - White lists identify allowed sites or content. - Black lists identify disallowed or blocked content. - Category levels use classification to block content based on content type. - Common methods for restricting content include: - Categorization of the content (such as sport sites, gambling sites, etc.) - URLs - DNS - *Parental controls* is content filtering software used by parents at home to monitor and restrict child web access. - Content filtering software can be expanded to include email, instant messaging, and other applications in addition to web content. - Most internet content filters can also block pop-ups and filter spam. - Keyword filtering can be configured to block the results of searches on specific words.
Network Access Control (NAC)	Network Access Control (NAC) controls access to the network by not allowing computers to access network resources unless they meet certain predefined security requirements. - NAC attempts to unify endpoint security by defining the security measures that must be in place for a computer requesting access to the network. - NAC requires a NAC agent (software to monitor the health of a machine) to be installed on each computer as part of the security requirements for computers attempting to gain access. - A client determined healthy by the NAC agent is given access to the network. - An unhealthy client (one that has not met all the checklist requirements) is either denied access or can be given restricted access to a remediation network, where remediation servers can help the client become compliant. - NAC is often used with 802.1x as an authentication protocol for port-based security. In addition to meeting authentication requirements, the client must also meet health requirements before access will be granted through 802.1x. - Microsoft's version of the NAC security tool is Network Access Protection (NAP).
All-In-One Security Appliance	All-in-one security appliances combine many security functions into a single device. All-in-one security appliances are also known as unified threat security devices or web security gateways. This type of device may be the best choice for: - A small company without the budget to buy individual components. - A small office without the physical space for individual components. - A remote office without a technician to manage the individual security components. Security functions in an all-in-one security appliance can include: - Spam filter - URL filter - Web content filter - Malware inspection - Intrusion detection system

	In addition to security functions, all-in-one security appliances can include: ▪ Network switch ▪ Router ▪ Firewall ▪ Tx uplink (integrated CSU/DSU) ▪ Bandwidth shaping
Application-Aware Devices	An *application-aware* device has the ability to analyze and manage network traffic based on the application-layer protocol that created it. Some of these devices can also apply quality of service (QoS) and traffic-shaping rules based on the application that created network traffic. Consider the following examples: ▪ An application-aware firewall can enforce security rules based on the application that is generating network traffic instead of the traditional port and protocol. ▪ An application-aware IDS or IPS can analyze network packets to detect malicious payloads targeted at application-layer services (such as a web server). ▪ An application-aware proxy manages traffic based on the application-layer protocols they support, such as FTP or HTTP. This allows the proxy to perform two key functions: ▪ Prevent the application client from performing undesirable actions. For example, an FTP proxy could be configured to allow FTP clients to perform downloads but inhibit uploads. ▪ Improve application performance. For example, an HTTP proxy can be configured to cache frequently accessed web pages.