5.8.4 Web Threat Protection Facts

A web threat is any threat that uses the internet to perform some sort of malicious activity. As web attacks become increasingly sophisticated, it is difficult for users to discern legitimate sites, valid links, and safe downloads. Because web threats can wreak so much havoc, organizations are turning to solutions that stop threats before they reach users.

Administrators must choose between using an all-in-one device that provides a one-stop shop for security protection, or using dedicated devices for each specific type of threat protection. The choice normally depends on the size of an organization and how much you want to spend.

The following table describes protections against web threats by using both hardware and software solutions:

Protection	Description
Website/URL Content Filtering	Website and content filtering prevents a user from visiting restricted websites. - Specific websites are identified as restricted; employees will not be able to view the sites on their browsers. - Website filtering can be used to enforce the organization's internet usage policy. - Website filtering helps to increase bandwidth availability.
Web Threat Filtering	Web threat filtering prevents a user from visiting websites with known malicious content. - It maintains a list of websites with known malicious content. - The websites on the list are blocked. - An administrator can monitor sites that have become infected with spyware or other malware, and can add those websites to the list.
Gateway Email Spam Filters	Gateway email spam filters prevent spam emails from reaching your network, servers, and computers. Spam filters can be configured to block specific senders, emails containing threats (such as false links), and emails containing specific content.
Virus Scanners	Virus scanners identify infected content and dispose of it. They are often coupled with email scanners.
Anti-Phishing Software	Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.
Data Loss Prevention	A type of software that protects sensitive data from being exposed.
Encryption	Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it.
Proxies	There are several types of proxies that are used to prevent web threats. - Transparent proxies are located between a user and the internet, and can redirect requests without changing the request. These can be used for web filtering. - Forward proxies can be used to filter web content, but can also be used to mask a user's identity for anonymity. This can make it difficult for attackers to target users or an organization. - Reverse proxies can be used for caching and authentication.