Summary of Cisco IOS Firewall

IOS Firewall is firewall functionality that is included within specific feature licenses of the Cisco IOS. Cisco IOS is the operating system that most Cisco devices operate. All routers, including the new Integrated Services Routers (ISR) run Cisco IOS. Cisco IOS has had a form of firewalling included since the very early releases. This was in the form of packet-filtering technology. This was the first generation of firewall technology. Packet filtering is implemented in Cisco IOS by what Cisco calls access lists. Nearly all Cisco routers in service will have access lists configured, because they are very flexible in their use. For example, you can use an access list to restrict who can connect to your router over both Secure Shell (SSH) and HTTP Secure (HTTPS) for management purposes; you can use an access list to restrict routing updates that are propagated from the router, or received by the router; and of course, you can use them on an interface to permit or deny specific traffic based on the configuration of the access list. An early improvement on access lists was the addition of the **established** command. The **established** command is used in an access list as shown here: Router(config)# access-list 100 permit tcp any host 192.168.1.1 eq established This access list permits any TCP connection from anywhere with the destination of 192.168.1.1 as long as it is what is called an established connection. This type of access list is good to place inbound on an external interface to get around the issue of dynamically allowing return traffic to clients. However, because the router is not tracking the state of the firewall, this does not really fall under the term of a stateful firewall. It is merely filtering packets, albeit ones with the ACK bit set in the TCP header. The first releases of Cisco IOS Firewall implemented a true stateful firewall that ran on a router. This functionality was known as Context-Based Access Control (CBAC). CBAC is the basis of the IOS Firewall and has now evolved into the IOS Classic Firewall. **The Cisco IOS Firewall is made up of three main features:** - Classic IOS Firewall - IOS Application Firewall - IOS Zone-Based Firewall **These features provide the following benefits:** - Stateful traffic inspection protects against worms, malicious users, and DoS attacks. - HTTP application inspection controls the security policy to limit web traffic vulnerabilities. - Instant messaging and other peer-to-peer application inspection controls offer policy application to prevent network resource abuse and reduce liability exposure. - Interoperates with Network Address Translation (NAT) to conserve and simplify network address use. - Simplified configuration using the Security Device Manager (SDM) that is available on most hardware platforms. - Virtual private network (VPN) routing/forwarding (VRF)-aware capability adds firewall functionality to multiple overlapping address spaces on the same router.