Cisco Secure Firewall 7.x

Discover key features

Capability	New Features	Post 7.x	Pre 7.x How does 7.x compare to previous versions?
Simplified Automation and Dynamic Policy Management	Dynamic Objects Dynamic Attributes Connector	These features enable robust policies in environments where fixed IP addresses don't exist. The Dynamic Objects can be updated without having to edit or redeploy the Access Control Policy multiple times. Think about AWS, VMware NSX, Azure or any other dynamic environments!	Previously, re-deployment of each change made on objects in the Access Control Policy was time-consuming and inefficient. Now you can utilize API or the Cisco Dynamic Attribute Connector to update constantly-changing objects in near real-time.
Secure Remote Worker	Dynamic Access Policy (DAP) Hostscan Custom Attributes: Per App VPN, Dynamic Split Tunneling, Deferred Update Multi-Cert Authentication SAML attributes support in DAP SAML + VPN Load Balancing Local Authentication for RAVPN	The features bring significant improvements around Remote Access VPN (RAVPN), eliminating the obstacles to increase NGFW adoption, and leading to a smoother migration from ASA to NGFW.	In previous releases, some key RAVPN functionalities like Dynamic Access Policy (DAP) or Load Balancing were missing. Also, there were concerns around the security posture of VPN enviroments that lacked NGFW capabilities. Now with Secure Firewall 7.x you can consolidate robust RAVPN capabilities with NGFW functionalities in a single box solution.
Superior Threat Visibility, Analytics and Logging	Snort 3 Unified Real Time Event Viewer SecureX Ribbon Integration	Snort3 provides a fully re-architected IPS engine for the Cisco Secure Firewall Portfolio. The new Unified Real Time Event Viewer, powered by advanced content filtering, provides a simple view of all security events. It streams data from sensors and correlates events, leading to faster investigations. SecureX Ribbon enables SecOps teams to pivot from any event seen in the Firewall to the SecureX platform, correlating data across the entire SecureX integrated ecosystem.	An evolution of the already robust intrusion detection engine Snort2, Snort3 provides up to 60% higher throughput, increased efficacy, and simplified policy management. In previous releases, searching and correlating events required to move between different tabs and was often cumbersome. Now with Unified Events, the entire flow of communication and all events triggered from it can be seen in one single view. Moreover, the Go Live option introduced in version 7.x allows to analyze events in real-time. Adding SecureX Ribbon on top of the mentioned features makes the Cisco Secure Firewall fully integrated with the wider Cisco Security Portfolio.
Accelerating Cloud Adoption	Secure Firewall Cloud Native in AWS ASAv and FTDv new platforms	The new Secure Firewall Cloud Native uses Kubernetes for orchestration to protect cloud workloads, with auto-scaling, auto-healing and real-time responsiveness to demand - especially useful in VPN deployments. The new release introduces OpenStack support for our virtual products (ASAv/FTDv/FMCv), launching a tiered licensing model, and a brand new FTDv instance with increased throughput up to 15.5 Gbps.	Previously, the only way to scale up and use cloud-native capabilities was to develop custom automation workflows, making it harder to deploy, orchestrate and manage the virtual firewalls. Now, the Secure Firewall Cloud Native uses Kubernetes to provide scalability and resilience, allowing customers to focus on achieving their business goals. The changes made to the virtual portfolio have unlocked a flexible licensing model, allowing customers to acquire licenses depending on throughput requirements on a wide range of platforms.

Learn more about Cisco Secure Firewall

cisco SECURE