The following table lists different firewall appliances.

| **Firewall** | [**License**](https://en.wikipedia.org/wiki/Software_license) | **Cost** | [**OS**](https://en.wikipedia.org/wiki/Operating_system) |
| --- | --- | --- | --- |
| [**Clavister**](https://en.wikipedia.org/wiki/Clavister) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on all Clavister NGFWs | Proprietary operating system cOS Core |
| [**Check Point**](https://en.wikipedia.org/wiki/Check_Point) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on Check Point security gateways | Proprietary operating system [Check Point IPSO](https://en.wikipedia.org/wiki/Check_Point_IPSO) and Gaia ([Linux](https://en.wikipedia.org/wiki/Linux)-based) |
| [**FortiGate**](https://en.wikipedia.org/wiki/Fortinet#FortiGate_Firewall_Platform) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on all Fortigate devices | Proprietary, FortiOS |
| [**Palo Alto Networks**](https://en.wikipedia.org/wiki/Palo_Alto_Networks) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on Palo Alto Networks firewalls | Proprietary operating system PANOS |
| [**Sophos**](https://en.wikipedia.org/wiki/Sophos) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on Sophos UTM | [Linux](https://en.wikipedia.org/wiki/Linux)-based appliance |
| [**Cisco ASA Firepower**](https://en.wikipedia.org/wiki/Sourcefire) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on all CISCO ASA devices | Proprietary operating system |
| [**Cisco PIX**](https://en.wikipedia.org/wiki/Cisco_PIX) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on all CISCO PIX devices | Proprietary operating system |
| [**Juniper**](https://en.wikipedia.org/wiki/Juniper_Networks) **SSG** | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on Netscreen security gateways | Proprietary operating system [ScreenOS](https://en.wikipedia.org/wiki/ScreenOS) |
| [**Juniper**](https://en.wikipedia.org/wiki/Juniper_Networks) **SRX** | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on SRX security gateways | Proprietary operating system [Junos](https://en.wikipedia.org/wiki/Junos) |
| [**Sonicwall**](https://en.wikipedia.org/wiki/Sonicwall) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included on Dell appliance | Proprietary operating system [SonicOs](https://en.wikipedia.org/w/index.php?title=SonicOs&action=edit&redlink=1) |
| [**Barracuda**](https://en.wikipedia.org/wiki/Barracuda_Networks) **Firewall** | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included Firewall Next Generation appliance | [Windows](https://en.wikipedia.org/wiki/Windows)-based appliance embedded firewall distribution |
| [**Cyberoam**](https://en.wikipedia.org/wiki/Cyberoam) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included Firewall Sophos appliance | [Windows](https://en.wikipedia.org/wiki/Windows)-based appliance embedded firewall distribution |
| [**D-Link**](https://en.wikipedia.org/wiki/D-Link) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Included Firewall DFL | [Windows](https://en.wikipedia.org/wiki/Windows)-based appliance embedded firewall distribution |
| [**Endian Firewall**](https://en.wikipedia.org/wiki/Endian_Firewall) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) | Free / Paid | [Linux](https://en.wikipedia.org/wiki/Linux)-based appliance |
| [**OPNsense**](https://en.wikipedia.org/wiki/OPNsense) | [Simplified BSD / FreeBSD License](https://en.wikipedia.org/wiki/BSD_licenses#2-clause_license_.28.22Simplified_BSD_License.22_or_.22FreeBSD_License.22.29) | Free / Paid | [FreeBSD](https://en.wikipedia.org/wiki/FreeBSD)-based appliance firewall distribution |
| [**pfSense**](https://en.wikipedia.org/wiki/PfSense) | ESF/[Apache 2.0](https://en.wikipedia.org/wiki/Apache_2.0) | Free / Paid | [FreeBSD](https://en.wikipedia.org/wiki/FreeBSD)-based appliance firewall distribution |
| [**Untangle**](https://en.wikipedia.org/wiki/Untangle) | [GPL](https://en.wikipedia.org/wiki/GPL) | Free / Paid | [Linux](https://en.wikipedia.org/wiki/Linux)/[NanoBSD](https://en.wikipedia.org/wiki/NanoBSD%22%20%5Co%20%22NanoBSD)-based appliance firewall distribution |
| [**Zeroshell**](https://en.wikipedia.org/wiki/Zeroshell) | [GPL](https://en.wikipedia.org/wiki/GPL) | Free / Paid | [Linux](https://en.wikipedia.org/wiki/Linux)/[NanoBSD](https://en.wikipedia.org/wiki/NanoBSD%22%20%5Co%20%22NanoBSD)-based appliance firewall distribution |
| [**SmoothWall**](https://en.wikipedia.org/wiki/SmoothWall) | [GPL](https://en.wikipedia.org/wiki/GPL) | Free / Paid | [Linux](https://en.wikipedia.org/wiki/Linux)-based appliance embedded firewall distribution [[4]](https://en.wikipedia.org/wiki/Comparison_of_firewalls#cite_note-4) |
| [**WinGate**](https://en.wikipedia.org/wiki/WinGate) | [GPL](https://en.wikipedia.org/wiki/GPL) | Free / Paid | [Windows](https://en.wikipedia.org/wiki/Windows)-based appliance embedded firewall distribution |

Firewall rule-set advanced features comparison[[edit](https://en.wikipedia.org/w/index.php?title=Comparison_of_firewalls&action=edit&section=4" \o "Edit section: Firewall rule-set advanced features comparison)]

| **Can:** | **work at OSI Layer 4 (stateful firewall)** | **work at OSI Layer 7 (application inspection)** | **Change TTL? (Transparent to traceroute)** | **Configure REJECT-with answer** | **DMZ (de-militarized zone) - allows for single/several hosts not to be firewalled.** | **Filter according to time of day** | **Redirect TCP/UDP ports (port forwarding)** | **Redirect IP addresses (forwarding)** | **Filter according to User Authorization** | **Traffic rate-limit / QoS** | **Tarpit** | **Log** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**Sidewinder**](https://en.wikipedia.org/wiki/Secure_Computing) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| [**Untangle**](https://en.wikipedia.org/wiki/Untangle) | Yes | Yes (Some modules) | No | No | Yes | Yes (With Policy manager) | Yes | Yes | Yes | Yes | Yes | Yes |
| [**WinGate**](https://en.wikipedia.org/wiki/WinGate) | Yes | Yes | Yes | No | Yes | Yes | Yes | No | Yes | Yes | No | Yes |
| [**Zeroshell**](https://en.wikipedia.org/wiki/Zeroshell) | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| [**pfSense**](https://en.wikipedia.org/wiki/PfSense) | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |

Many firewall vendors offer [next-generation firewalls](https://searchsecurity.techtarget.com/feature/Six-criteria-for-buying-next-gen-firewalls), but they argue over whose technique is best. A next-generation firewall is [application-aware](https://searchnetworking.techtarget.com/tip/Application-layer-firewalls-defend-against-attacks-up-the-stack). [Unlike traditional stateful firewalls](https://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls), which deal in ports and protocols, [next-generation firewalls](https://searchnetworking.techtarget.com/news/2240187725/Hughes-melds-WAN-accelerator-Fortinet-security-in-new-gateway) drill into traffic to identify the applications traversing the network. With current trends pushing applications into the public cloud or to be outsourced to Software as a Service (SaaS) providers, a higher level of granularity is needed to ensure that the proper data is coming into the enterprise network.

Each vendor has its own approach to building [application awareness](https://searchdatabackup.techtarget.com/answer/How-application-awareness-in-backups-increases-productivity) into a firewall. SearchNetworking.com asked each of the leading firewall vendors to explain [how their next-generation firewalls differ](https://searchnetworking.techtarget.com/tip/Network-management-next-gen-firewall-tools-take-center-stage) from the competition. Here is what we learned.

* [Astaro](http://www.astaro.com/) uses an application signature database from its partner Vineyard Networks to [deliver application awareness](https://searchdatabackup.techtarget.com/tip/Application-awareness-comes-to-hypervisor-snapshots) to its Astaro Security Gateway. Through this partnership, Astaro's firewall can distinguish different applications running from the same website and apply [Quality of Service](https://searchunifiedcommunications.techtarget.com/definition/QoS-Quality-of-Service) options to prioritize and allocate bandwidth to these applications.  The latest version of Astaro Security Gateway enhances the presentation of this information to the firewall administrator. It offers a network-wide view that allows administrators to quickly define security polices based on the real-time situations. The key, according to Astaro, is to enable IT to react to new threats by seeing what is happening and fine tuning the firewall quickly and easily.

Astaro is also focused on identifying new, unknown application types as soon as new applications start hitting customer networks. Planned for an upcoming release, the system would allow administrators to opt-in and anonymously submit unknown packet types for review by Astaro engineers. The company will use the compiled data to identify these applications and add them to the signature database.

* [Check Point Software](http://www.checkpoint.com/) has developed the AppWiki application library, which the company claims can identify over 5,000 applications and 100,000 social networking widgets. These application signatures are pulled into the company’s Check Point Application Control and Identity Awareness Software Blades. The software also integrates with [Active Directory](https://searchwindowsserver.techtarget.com/definition/Active-Directory) to identity the user and endpoint, allowing administrators to customize granular security policies. [Check Point](https://searchsecurity.techtarget.com/feature/Check-Point-Mobile-Access-Software-Blade-SSL-VPN-product-overview) also offers the ability to educate users in real time. Agent software on the user's PC, UserCheck, will pop up a window when the user violates security policy. The window explains the violation and guides users through remediation. This software also lets users provide feedback to administrators, streamlining the process of customizing security policies in response to user needs.
* [Cisco Systems](https://www.cisco.com/) has announced plans to add new levels of application visibility into its Adaptive Security Appliance (ASA), as part of its new [SecureX security architecture](https://searchnetworking.techtarget.com/news/2240032226/New-Cisco-network-security-architecture-has-next-generation-firewall). Cisco claims that this new architecture will not only address application awareness, but also user and device identification, as it rolls out features throughout 2011. Details on how Cisco acquires that application visibility remain sketchy for now.
* The [application control](https://searchenterprisewan.techtarget.com/feature/Bringing-application-control-and-awareness-to-micro-branches) functions of [Fortinet’s](https://www.fortinet.com/) FortiGate devices use protocol decoders and decryption of network traffic to identify applications. The company’s FortiGuard Labs team maintains an application signature database, adding signatures for new applications as well as updating signatures for new versions of existing applications. The application database enables [Fortinet’s products](https://searchnetworking.techtarget.com/tip/Next-gen-firewall-reviews-Fortinet-FortiGate-3950B) to separate disparate applications from a single site, such as Facebook or Google, and allows separate policies for each. Fortinet claims that its products have a performance and integration advantage over its competitors because all of its technologies are developed in-house.
* [Juniper Networks](http://www.juniper.net/) uses a suite of software products, known as AppSecure, to [deliver next-generation firewall](https://searchnetworking.techtarget.com/news/2240214283/New-modular-PA-7050-Palo-Alto-firewall-scales-to-120-Gbps) capabilities to its SRX Services Gateway. The application-aware component, known as AppTrack, provides visibility into the network based on Juniper’s signature database as well as custom application signatures created by enterprise administrators. With AppTrack providing visibility, the AppFirewall and AppQoS components of the suite provide the policy enforcement and traffic control of the applications. Juniper also claims a high level of scalability in its platform, with the ability to deliver application protection at up to 100 Gbps speeds.
* [McAfee](https://www.mcafee.com/en-us/index.html), recently acquired by Intel,  uses its McAfee AppPrism technology for application discovery and awareness in McAfee Firewall Enterprise. AppPrism identifies thousands of applications, regardless of port or protocol, backed by application signatures developed in-house by McAfee’s own Global Threat Intelligence team, the company claims. AppPrism also provides a high level of application control, allowing administrators to disable just the riskier portions of an application. For example, administrators can use the technology to block the file sharing capabilities of an instant messaging application without blocking a user's ability to chat. McAfee claims its next-generation firewall has an edge because its application-awareness technology is a core part of its firewall architecture and all components, including application signatures, all of which are internally developed.
* [Palo Alto Networks](http://www.paloaltonetworks.com/) says it was the first vendor to deliver next-generation firewalls and the first to replace port-based traffic classification with application awareness. The company’s products are based on a classification engine known as App-ID. App-ID identifies applications using several techniques, including decryption, detection, decoding, signatures and heuristics. Individual App-IDs for a given application can rely on any combination of these techniques in a single bundle, allowing the engine to identify all versions of an application, as well as all of the platforms the application runs on. App-ID, as the core of Palo Alto’s firewalls, is always running, so it can identify when an application performs a function, such as a file transfer, and it can apply policy to that specific function. The company also notes that App-ID is extensible, so that as new techniques become available, they can be incorporated into the classification engine.
* For [SonicWALL](https://www.sonicwall.com/solutions/next-generation-firewall/), the formula for application awareness in its Next-Generation Firewall is a combination of Deep Packet Inspection (DPI) and an ever-expanding signature database that can currently identify and control upward of 3,500 applications and application functions. SonicWALL's Reassembly-Free Deep Packet Inspection (RFDPI) scans every packet across every protocol and interface. On the signature side, the the SonicWALL Research Team continually generates new signatures, which are automatically delivered and implemented without requiring extra work from the network administrator. In addition, IT shops can create their own signatures as needed.

SonicWALL's [firewall solution](https://searchsecurity.techtarget.com/definition/firewall) also includes a Visualization Dashboard and Real-Time Monitor, which enables administrators to see specific applications on the network, including information on who is using them and to what extent they're being used. The idea is to use this information for policy setting and troubleshooting.