The traditional firewall can prevent some malicious traffic within a network. However, technology is advancing rapidly so the conventional firewall is not enough. The term “next-generation firewall” is taking over the internet, but what does it truly mean? A next-generation firewall adds some additional features to the normal firewall. Application control, IPS, advance threat prevention, and URL filtering are some of the additional features.

There are many differences between a traditional firewall and a next-generation firewall. For security dealers to keep up with current threats, it is very important for them to know why next-generation firewall are important and what features they must have.

While choosing a next-generation firewall, we should specifically look for these five features:

1. **Application Awareness**

An important difference between the traditional firewall and the next-generation firewall is that the latter has application awareness. While the former depends on ports to determine the type of application, the next-generation firewall is port independent. The [security](http://www.cardzgroup.com/ContactLessSmartCard.html) of a next-generation firewall is better, as it can identify applications regardless of their ports and protocols. Furthermore, it can allow, block, or limit, access to an application without bothering about its protocols.

1. **Identity Awareness**

Similar to application awareness, identity awareness also plays an important role in security. You will find all major authentication protocols in the next-generation firewall such as LDAP, RADIUS, etc. Thus, it does not only control the type of traffic entering the network; it also manages what specific users can send and receive. You get granular control of your application as you specify the group of users who can use it.

1. **Better Management**

We can get centralized management with the help of the next-generation firewalls. A business’s logging and reporting department can use the tools of this firewall to improve management. Not only this, administrators can get a better log analysis. Furthermore, they can export the rules and configuration of your firewall to get centralized management. The security health dashboard gives a clear picture of the traffic patterns. Not only this, but one can also find associated risks in real-time. You can automate routine tasks, employ shortcuts, reuse elements, and employ drill-downs. Thus, you can improvise maximum efficiency with minimal effort.

1. **Integrated Intrusion Prevention System**

Integrated IPS is the limelight of a next-generation firewall. You can always spot the difference between a traditional firewall and a next-generation firewall with the help of IPS. When we deploy a traditional firewall, the IPS or Intrusion Detection System (IDS) also get deployed. However, this was being done with the help of a separate appliance. IDS or IPS can be completely integrated in the next-generation firewall and it can be activated or deactivated according to your needs. You may think that the functionality of IPS is the same in traditional and next generation firewall. However, the performance and accessibility of information are better with next-generation firewall IPS.

1. **State-full Information**

Another prominent feature of the next-generation firewall is its state-full information. You may not feel any general difference between the stateful information of traditional and next-generation firewalls. However, the former can only track the traffic from layer to layer four. A next-generation firewall can detect traffic from layer two to layer seven. In some cases, the detection may expand till layer eight because of identity awareness. State-full information plays an important role in providing you more control of your traffic. You can also implement very granular policies with this feature of the next-generation firewall.

**Conclusion**

As system integrators, one can always implement a better next-generation firewall after understanding its full features. Moreover, you can ensure the network security of your organization when you realize the importance of the next-generation firewall.