



# Advanced Computer Engineering Services

## Making Your Vision a Reality!

[www.aces4hire.com](http://www.aces4hire.com)

Custom Software Development • Complete Internet Solutions  
Graphic Design • Copy Writing & Advertising

---

---

### FIGHT THE ENEMY WITH FIRE

A firewall is a security apparatus which prevents unauthorized users from accessing a computer network and monitors transmission of information into and out of a network. It is the most essential tool to curb viruses and worms, and it clamps down on the amount of unwanted spam received by the network's clients. Service providers generally offer the 'Stateful Inspection' mode and sometimes also add the 'Deep Inspection' mode to the firewall. Traditionally, firewall systems and basic anti-virus software used to provide adequate coverage for networks from curious and unwanted visitors. However, the increasing knowledge and innovative technology of modern hackers allows them to penetrate even the most resolute firewalls. Thus, security issues need a more holistic approach, and firewalls need to be supplemented with an additional layer of security such as 'Intrusion Detection'. This will facilitate the process of screening internet traffic detection. As soon as the firewall detects whether traffic can gain access to a computer, the 'Intrusion Detection System' will thoroughly check it to examine and identify any suspicious attack pattern. If an attack pattern is detected as suspicious, then the traffic is automatically and immediately terminated. Thus 'Stateful' or 'Deep Inspection' firewall systems supported by IDS can satisfactorily prevent hackers from transporting spam or viruses to the network client's machines. A layered security approach enables administrators to protect the communications and resources at the perimeter and infrastructure, as well as extended to remote sites and users.

The network security services companies offer customized security solutions according to the specific needs of their clientele. Integrated Firewall/IPSec VPN appliances and systems incorporated with anti-virus features ensure that there are no weak links in the network. A 'Stateful' system empowers the administrators to effectively control the accessibility of the network and also authenticates identities as given by the surfers to minimize unauthorized roaming and keep hackers at bay. Firewalls collect information on various details in a packet header— source and destination IP addresses, source and destination port numbers, packet sequence numbers, etc. The device then continuously monitors the state and position of each TCP session or UDP pseudo-session navigating the firewall, performing TCP reassembly as and when necessary, thus ensuring accurate interpretation of the communication session. As soon as a responding packet arrives, the firewall readily compares the information reported in its header with the corresponding state of its associated session stored in the inspection table. If they are identical, then the responding packet is allowed to pass the firewall. If the packet does not match, then it is immediately stopped in its tracks.

The 'Deep Inspection' firewall adds muscle to the 'Stateful Inspection' and integrates intrusion prevention technology into a system to prepare application-level attack protective shields at the perimeter of a network. Leveraging the efficiencies of both technologies, the Inspection firewall can competently perform network security functions as well as analyze the application message to determine the right to passage of the traffic. Deployed at the perimeter, a Deep Inspection firewall concentrates on averting application-level attacks aimed at Internet-facing applications, such as Web, e-mail, FTP and DNS.

Firewalls also introduce network segmentation to contain attacks in the clients' infrastructure. The machines of the clients withstand the system overloads with the help from strong and reliable 'Denial-of-service'/'DoS' protection service of the security provider. Apart from the mentioned

'DoS' attacks, a quality firewall system must also shield the network client from application-level attacks and secure wireless LANs, consolidate firewall deployments to maintain a consistent performance. The IPSec VPN system allows companies to establish secure connections between management, business partners, employees and customers, thus in a nutshell providing an end-to-end blanket security solution. The dynamic and secure VPN combines the efficiency and resilience of the route-based VPN with the security and the flexibility of a policy based customized firewall.

The Integrated Firewall/VPN system can be managed by using the following - Command Line Interface (CLI), a web based graphical user interface or through a centralized management console, which simplifies configuration, deployment and continuous management. The above-mentioned services are available at almost all quality network security providers but firewalls can be seriously detrimental to Internet Video Communications. It can involuntarily block video sessions resulting in frustration as well as on possible sources of revenue because of lost business opportunities. **ACES** has the technology to provide seamless video delivery between different combinations of firewalls and modems. The Firewall/VPN and IPSec services of **ACES** has been certified by the ICRA for conforming to its common criteria, ensuring world class and absolutely safe standards.

So if you are experiencing a deluge of spam and afflicted regularly by stubborn viruses intent on wrecking your machine, then **click here** to put an end to your concerns.