10 things to know when choosing a hardware firewall

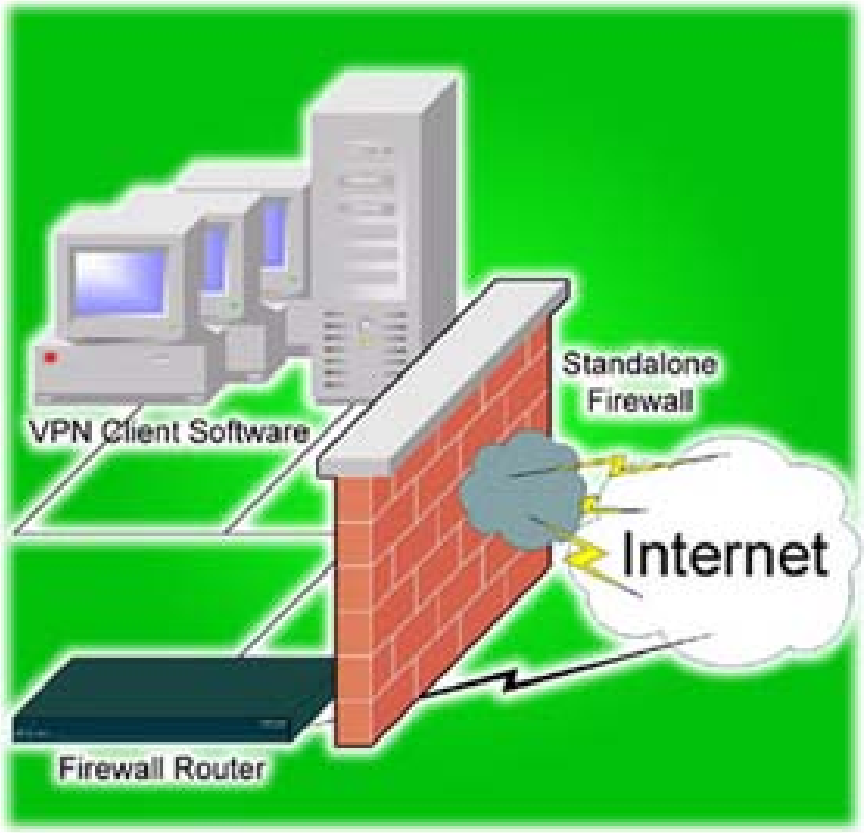
When you choose a hardware firewall, consider the following 10 factors to ensure that your business gets the most out of investment, security, and productivity.

Network Administration - Today's firewall plays an important role in protecting an organization's network from an almost endless list of attacks coming from the Internet. The choice of firewall also often determines how remote locations connect to central systems to access the necessary resources or to perform important tasks easily. When you choose a hardware firewall, consider the following 10 factors to ensure that your business gets the most out of investment, security, and productivity.

1. Reliable security

For a wide range of enterprise models, some network security devices need to have a range of features and services, so they cost quite a bit, while some other firewalls quit. take the necessary services to lower costs.

To ensure a good and reliable foundation is chosen. Barracuda, Cisco, SonicWALL and WatchGuard are the brands that make up the majority of the market share because they provide reliable security. For any brand you choose, confirm that the firewall is ICSA certified, which is an industry standard for package inspection.



2. Accessibility

Multinational enterprises often require excessive security control, but even organizations that need such high protection do not have to restrict themselves to devices that are only configured with the command line. Many firewall models deliver tight security and provide a user-friendly administration interface (GUI).

There are several benefits to the user interface here, the GUI helps to avoid installation errors. GUI makes it easier to diagnose and troubleshoot. The GUI also makes it easier to train employees and make changes, upgrades and replacements.

When choosing a hardware firewall, what you should consider is accessibility. The easier it is to administer a platform, the less specialized it is to install, maintain, and troubleshoot that platform.

3. Support VPN

The purpose of a firewall is not just to prevent hackers and traffic from being verified. An effective firewall can also set and check secure channels, allowing remote connections. Therefore, you should look for hardware firewalls that support both SSL and IPSec protected VPN connections from devices of the same type (for site-to-site or site-to-site VPNs) as well as other Secure connection from mobile employees.

4. Capacity

Firewalls, thanks to their networking roles, typically serve as an Internet gateway for an organization. Smaller offices can increase the capacity of a firewall to achieve dual capacity for use as a security device and a network switch. Meanwhile, larger organizations often configure firewalls into a larger architecture so that the firewall only serves as a traffic filtering function.

Make sure the firewall can manage the assigned loads. This means that it needs to have an appropriate Ethernet port number and proper speed (10Mbps / 100Mbps or 1000Mbps if necessary). However there are many other problems. Make sure that the firewall you choose or maintain has the CPU capacity needed to perform packet inspection, perform port security and routing functions.

Attention should be paid to the manufacturer's recommendations for maximum button support. If you exceed the capacity of a router, you will receive errors, denial of traffic is often due to a lack of subscriptions or ineffective performance.

5. Technical support

Hardware error. That is the worst, sometimes a new device from the factory does not mean it will work properly. Check that 24 × 7 technical support is always available and make technical support contacts with the firewall manufacturer.

Before buying, call the manufacturer's technical support team and ask some questions about deployment and configuration. The quickness and accuracy of the support you receive will give you a good support service that you will get when your hardware fails at a certain stage.

6. Wireless security

Even if an organization does not believe this problem is necessary, you should also consider hardware firewalls with wireless networking capabilities. IT staff can deploy blocks with wireless services has been disabled. The cost of adding a new WLAN function to purchase may increase, even if guest access or the flexibility of the network is required, secure wireless connectivity only takes one click (not a purchase). New router completely). And when the needs of the organization change, the WLAN function may prove necessary.

7. Gateway security services

Many organizations successfully reduce costs by focusing their protection on viruses, spyware and spam using their firewalls. When comparing firewall capabilities and deciding the overall cost to be paid, the cost savings factor can be reduced if you deploy these services on a firewall device, compared to a transmission domain controller. system or other server.

8. Content filtering function

While many IT organizations are moving to OpenDNS for content filtering purposes, some firewall manufacturers still offer web filtering services. The advantage of this service is that all network services associated with the business, from gateway security services to content filtering, can be consolidated on one device. The downside is that you have to pay to get this privilege.

When evaluating hardware firewall solutions, consider the organization's needs and budget. Decide whether content filtering needs to be managed by the firewall. If the answer is yes, select a firewall that supports reliable and good content filtering.

9. Advanced testing and reporting functions

Firewalls manage important network tasks. During the process, a router can block intrusion attempts, detect attacks and record failures or failed connections. However, this information is useful for network administrators

only when it is available in readable format.

Searching for firewalls can not only check important events but also record that data in an appropriate format. A good firewall will generate minimal email alerts, which are also important events.

10. Automatic failover

Some organizations require automatic WAN failover or reserved Internet connections with automatic error detection and correction. However, many firewall models do not support automatic failover. If this feature is important to your organization, confirm that the model you choose must be capable of failover.

In addition, make sure the model you choose supports the failover methods that your organization will use.