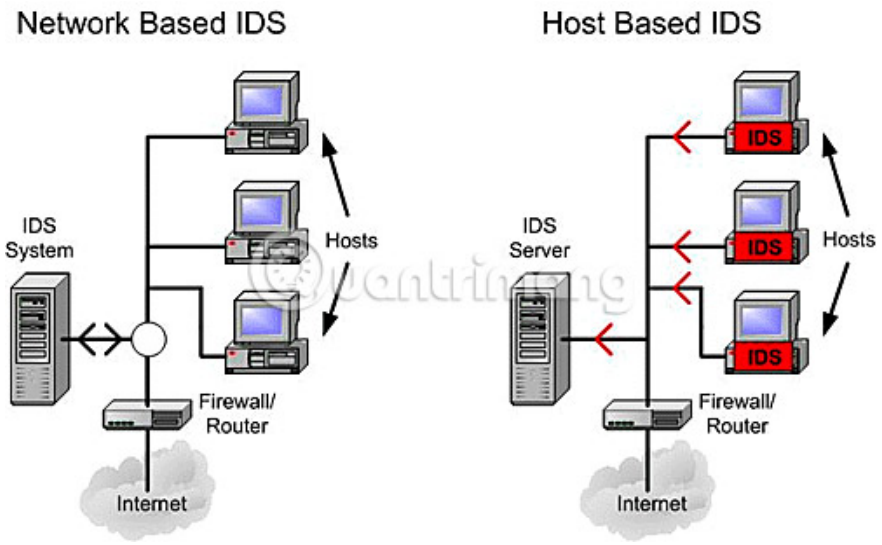
Host-based intrusion prevention

Layered security is a widely accepted principle in computer and network security. The basic premise of this principle is that it requires multiple layers of defense to protect resources and data against multiple attacks,

Layered security is a widely accepted principle in computer and network security. The basic premise of this principle is that it needs multiple layers of defense to protect resources and data against multiple attacks, as well as threats. Not only because a product or a technique cannot resist any possible threat, but having multiple defense lines also allows a product to 'catch' the 'intruders' to overcome the outside defense.

Many applications and devices can be used for different security classes, such as antivirus software, firewalls, IDS (Intrusion Detection Systems or Intrusion Detection Systems), etc. Each type is available. The function is slightly different and has the ability to protect the system from a variety of different attacks.



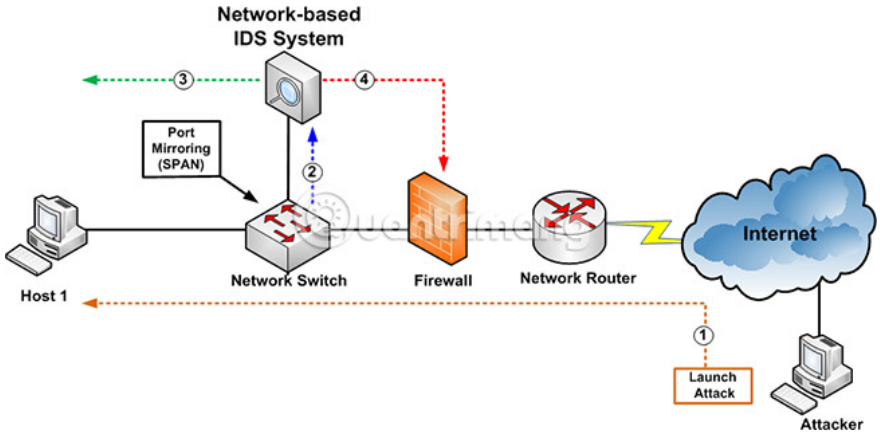
One of the newer technologies is IPS, or Intrusion Prevention System - Intrusion Prevention System. IPS is like a combination of IDS with a firewall. A normal IDS will record or warn users about suspicious traffic, but how it responds depends on the user. IPS has policies and rules for comparing network traffic. If any traffic violates these policies and rules, the IPS can be configured to respond instead of just alerting the user. Typical responses may be to block all traffic from the source IP address or block incoming traffic on that port to actively protect the computer or the network.

There is a network-based intrusion prevention system (NIPS) and a server-based intrusion prevention system (HIPS). Although it may be more expensive to deploy HIPS - especially in a large enterprise environment, server-based security is recommended whenever possible.

Host-based intrusion prevention solution (HIPS) for the network

1. **Do not rely on signature** (signature): Signature or specific characteristics of known threats is one of the primary means used by antivirus and intrusion detection software (IDS). Signature cannot be developed until the real threat exists and the user is likely to be attacked before the signature is created. Server-based intrusion prevention solutions should incorporate signature-based detection with unusual detection to set the baseline of "normal" network activity, then respond to any traffic looks unusual. For example, if the computer never uses FTP and suddenly some threat tries to open an FTP connection from the computer, HIPS will detect that this is an abnormal operation.
2. **Working with configuration** : Some HIPS solutions may be limited to programs or processes that they can monitor and protect. You should try to find a HIPS capable of handling commercially available packages as well as every custom home application in use. If you don't use custom applications or don't consider this an important issue for your environment, at least make sure that your HIPS solution protects running programs and processes.
3. **Allow creating policies** : Most HIPS solutions come with a fairly complete set of policies and suppliers will often have new policy updates or releases to provide specific feedback on threats. New threat or attack. However, it is important that you have the ability to create your own policy, in case there is a particular threat that the provider does not explain, or when the threat has just exploded and you need approval. books to protect their system, before the provider has time to release updates. You need to ensure that the products you use are not only able to allow policy creation, but creating that policy must also be easy to understand and do not require weekly training or professional programming skills.
4. **Provide centralized reporting and management features** : When it comes to server-based protection for individual servers or workstations, HIPS and NIPS solutions are relatively expensive and out of the user's ability. ordinary family. So, even when talking about HIPS, it might be worth considering from a HIPS deployment perspective on hundreds of desktops and servers on a network. Although it is great to be protected on a single desktop level, managing hundreds of individual systems or trying to create aggregate reports is nearly impossible without management and report good focus. When choosing a product, make sure it has centralized reporting and administration features that can deploy new policies for all machines or to generate reports from all machines in one location.

Other things to remember



There are a few other things you need to remember. First, HIPS and NIPS are not a simple solution to complex issues like security. They can be a great addition to a robust multi-layer defense system, including firewalls and antivirus applications, but cannot replace existing technologies.

Second, deploying an original HIPS solution can be a bit difficult. Configuring detection capabilities based on anomalies often requires a lot of 'assistance' for what the application understands "normal" traffic and what is abnormal traffic. You may experience some problems when setting the baseline to determine the "normal" traffic for the system.

Finally, companies often decide to buy products based on what it can do for them. In fact, this is measured based on either Return On Investment or ROI (return on investment). That is, if you invest a sum of money in a new product or technology, how long does it take for the product or technology to benefit itself?

Unfortunately, network security and computer products are often not the same. If the security product or technology works as designed, the network will be secure, but there will be no "profit" to measure ROI from there. Must look at the left side and consider how much the company can take if that product or technology is not applied. How much money is needed to rebuild the server, recover data, time and resources for the technician to 'clean up' after an attack, etc.? Without using that security product, it is likely that the business will lose far more than the cost of purchasing the product or technology.