
ENTERPRISE PLANNING:

INTRUSION PREVENTION SYSTEMS

Considerations before deciding upon an Intrusion Detection and Prevention System for your network

The last few years have seen a very prominent change in the information security arena. Most software vendors are now producing software with engraved security features. Application software houses are now injecting stringent processes to control the security of their product. Moreover it is well understood that operating systems and widely used application software will no longer carry bugs and vulnerabilities to be exploited.

Hence, attention will then turn towards self developed applications such as application web sites, enterprise production software etc. Common developers will also need to understand secure development, code writing and testing else they would turn into sitting ducks and wait to be compromised.

The wave of the future, *Intrusion Prevention Systems* are products that are beyond operating systems and are able to detect and can prevent lethal attacks against your operating systems as well as your custom applications.

In this paper we would discuss all the aspects of an Intrusion Prevention System that need to be considered before a product is selected. As intrusion prevention technology is relatively new hence there are several variants available in the space that provide similar functionality but may employ different underlying technologies. In the sections below we would discuss all the features that should be a part of a good intrusion prevention product.

Network Integration

Large enterprise networks are of two kinds some that have been designed before deployment and are designed to be modular, whereas the other where the growth of the network is ad-hoc and unplanned. Deploying an intrusion prevention system will usually change the network topology and hence the device should be flexible enough to fit into any of the described networks.

The device should have basic features such as Network Address Translation (NAT), Layer 2 Routing or Bridging and basic routing features. Features such as NAT and Bridge are required as some network are already protected using a device and may not require address translation and hence can run the more stealthy bridge configuration. Most networks require basic routing features to be able to efficiently route packets.

Transit Error Detection

Network traffic often flows through a routes that are un-maintained, these weak networks can induce errors in the packets flowing through them these erroneous packets are called mangled packets. Mangled packets most often go undetected into a network and can cause damage on system that are not capable of handling the exception. Attackers are also known to intentionally craft such packets to damage vulnerable systems.

Network traffic Normalisation is a very important feature that is often neglected from network security devices and hence is a must for an intrusion prevention device that is responsible for protecting the secured network from damage.

Packet Filtering

The Internet is largely contaminated with traffic that is meaningless and wasteful, moreover traffic of this kind is purposefully generated by attackers to probe computer

systems. Often attacks are launched on vulnerable services that run unshielded on a system. To prevent such needless traffic and malicious attacks one would need some device that would filter traffic and only allow legitimate traffic to flow to the system.

A stateful packet filtering firewall is a must have for a network to prevent malicious attacks and probes on critical infrastructure. Most facilities have firewall as a part of the network but having an integrated stateful firewall in an IPS is a definite plus as it provides complete integration and therefore is faster and easy to configure and manage.

OS Security

Operating systems form the largest targets for attackers, vulnerable software running on the OS allows attackers to compromise the system and run infecting software also called a backdoor. A backdoor allows the attacker easy access to the compromised host at any point in the future. As vulnerabilities are found on operating systems vendors release patches to mitigate the vulnerabilities. An attack on an un-patched system would succeed before a patch can be applied. Hence one needs some prevention technology that detects all attacks on a particular vulnerability even if the system hasn't been patched.

The Intrusion Prevention System should possess a complete backdoor detection kit that would prevent against any malicious usage of the protected system. It should be able to detect and prevent against different families of backdoors that operate on different technologies and propagation mechanism. An IPS should also be able to detect new vulnerabilities and all variants possible that attack the same vulnerability.

Application Security

As discussed in the sections above, application security will turn into the next

big threat faced by security solution providers. Operating systems will now be more secure and will be well tested before they are deployed. Common application software vendors are also using stringent software development processes that would in turn produce software that is more efficient and secure. Applications software that is developed without such processes which is usually the case with in-house software development projects will have hidden vulnerabilities that would sometime be found and exploited.

To cover such unseen threats one would need to understand commonly used application protocols such as HTTP, DNS, IMAP etc. These protocols are often used to build applications and hence to find anomalies in these protocols one would need to completely absorb the protocol standard and applications that use the standard. Intrusion prevention systems must possess application protocol inspectors that are able to bind the incoming traffic to a pre-set standard. Hence this technology will be extremely useful to detect and protect against unknown application attacks.

Denial of Service Attacks

DoS and Distributed DoS attacks are the only ones that the world has no answer to, these attacks flood the uplink lines with junk data and hence deny access to legitimate users. These attacks are often well co-ordinated and it is very difficult to identify the source of the attack. The most popular large websites have faced DDoS attacks in the recent past and have no answer to the issue.

An IPS should be able to reduce the risk of a DDoS if not mitigate it completely. Intrusion prevention systems must have an effective traffic anomaly detection system that is capable of detecting peaks in unwanted traffic. The traffic anomaly system should however be able to detect between legitimate and illegitimate traffic.

Capacity and Performance

Intrusion prevention systems will soon turn into the centrepiece of an organisations security armoury, therefore an intrusion prevention system should be able to handle a good amount of traffic and at the same time be able to scan all the traffic flowing through the system. Capacity of a device is defined in terms of megabits transferred per second through the device. This figure should exceed the maximum amount of data being transferred through the network.

Ease of Use

Intrusion prevention systems can be very complicated to configure and deploy, configuring an IPS usually requires additional expertise to be able to install and manage the device. This often can be additional burden on enterprises as quality administrators are rare to find and can be expensive.

For more product information visit www.netmonastery.com/products NetMonastery bridges the gap between traditional intrusion detection systems and the cutting edge prevention technologies. The difference is in the detection technologies used and the extended attack recognition systems that are built only for the intrusion prevention space and may not be relevant in the intrusion detection space.

Global Headquarters

F - 109, Kailash Industrial Complex, Park Site,
Vikhroli (west), Mumbai 400079, INDIA
Tel: +91 22 30965080
Email: sales@netmonastery.com



NetMonasteryTM
Monitoring Internet Security

Copyrights 2004 NetMonastery. All rights reserved worldwide

SiteVaxinPro is trademark of NetMonastery logo are registered trademark, of NetMonastery. All other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.