NIDS placement in the real world

I have yet to see anything that had recommendations for sensor placement and sensitivity. I use this as a guideline for Network Intrusion Detection System (NIDS) installs on my networks. As always, I take no responsibility if you use this and get hacked. It is provided as a guideline.

Priority and Placement

The first thing people ask when they decide they need a NIDS is "Which one?". The next question is "How much?". Sometime after they have worked out what they are buying and how much they are going to spend they get to the design phase.

How about we take a different approach and decide where sensors are going on our network and how many we need? During this process let's also put a priority on each sensor, so if our budget gets slashed we know where we can trim the cost. In a perfect world this wouldn't happen, but we all know how things really work. Here is a rule I use for giving sensors a priority.

"As the importance of the data being watched increases, the importance of the sensor increases."

My backend database is my most important server. I can't afford to not monitor this server. Devices outside my firewall are the least important. If they are outside the firewall, they must be hardened and secure and more than likely do not host valuable data. If we follow the rule, sensors near my database are the most important. The farther we move from the database server, the less important the sensors are. Sensors the farthest from the database are the first to go if the budget gets cut. This also means that if you can only afford one sensor, you want it as close as possible to your important data. If you can have two sensors, put one the next hop away from the first. I use hop here instead of network only because you may choose to put more than one sensor on a network.

Often administrators think they should put a sensor outside their firewall. I put my firewall up to prevent unauthorized access to my servers. If the firewall is doing its job, it should be blocking attacks. If it isn't, how does a sensor outside the firewall alert me to attacks on my database server? It doesn't. If I am successful in getting past the firewall, there is nothing to detect my attacks internally. Internal attacks are another reason to put the sensor near the database server. Again, the sensor outside the firewall can't detect attacks from employees or attackers that are able to get onto our internal network from inside. If my budget is small then it is likely I don’t have a lot of time to investigate attacks. The majority of alerts outside the firewall are port scans. If my firewall is blocking them, I don’t need to be alerted to every one. Firewall logs should be

enough and I can review them as time permits. My internal sensor will alert me to attacks that make it through the firewall and present a threat to my data.

A simple analogy

Credit to Kevin Brown for the following analogy. This should help reinforce the above rules.

Think of your network like a bank. Firewalls are like locks on the doors, and NIDS sensors are like cameras. Does a bank keep its cameras on the inside or outside? They are inside, pointing at the doors everyone walks through to get inside. Now the bank has a picture of everyone who passes through the doors, including employees. They also put cameras near the teller windows and vaults where the money, aka important data, is kept. The monitoring is as close to the source they are protecting as possible. A camera looking at your front doors, will tell you who tries the locks at night. If they manage to get in, your internal camera will record it. You aren't particularly concerned with people trying the locks. You know the doors are locked, so they can't get in. Your goal of protecting the money has been achieved.

Tuning

Tuning the sensors is an ongoing process; your job isn't complete after your IDS rollout is done. Each sensor will need to be adjusted to selectively watch and ignore network traffic. Every sensor should be different because of the data it is protecting and what kind of traffic it is watching. Sensors outside the firewall will be the least sensitive, because of the amount of traffic they see. The goal is to avoid false positives while also eliminating false negatives. Here is another rule for adjusting sensitivity.

"As the importance of the data being watched increases, the sensitivity of the sensor increases."

The sensor near my database server needs to be the most sensitive. A sensor placed outside the firewall will, most likely, mean a high number of false positives, so it will be the least sensitive. Sensors in the DMZ will be somewhere in between. This is where tuning will come into play. Adjustments can be made to ignore certain attacks or to adjust thresholds.

Summary

I haven't discussed management in the above rules. Management of the NIDS introduces a new factor to the puzzle. The tendency of administrators is to de-sensitize the NIDS until it doesn't produce false positives. While this does reduce alarms, it also defeats the purpose of the NIDS.

Security is a full time job. Managing an IDS is two full time jobs. The trick is to tweak things so that the IDS is an extension of your toolbox and it helps you defend your network against attack.

To review, if you don't have a large budget, the best use of your money is a sensor close to your data. With a larger budget, you place additional sensors farther from the sensitive data.

The discussion here is strictly about Network Intrusion Detection Systems. Host based solutions are beyond the scope of this document, but must not be discounted. A solid security policy uses every available resource for protecting systems and networks.

Jason Lewis
http://www.packetnexus.com/