Table of Contents

Intrusion Detection Systems ........................................................................................................................................... 2
IDS Characteristics ............................................................................................................................................................ 3
Passive and Active Detection ........................................................................................................................................... 5
Detection Methods ........................................................................................................................................................... 6
Detection and Inspection .................................................................................................................................................. 8
Network-Based IDS (NIDS) ............................................................................................................................................... 10
NIDS – Characteristics .................................................................................................................................................... 12
NIDS – Advantages .......................................................................................................................................................... 13
NIDS – Disadvantages ..................................................................................................................................................... 16
NIDS – Typical Deployment Environments ..................................................................................................................... 17
Intrusion Detection/Prevention System ......................................................................................................................... 18
IDS: Promiscuous-Mode ............................................................................................................................................... 19
IPS: Inline-Mode ............................................................................................................................................................ 21
IDS: Promiscuous-Mode .................................................................................................................................................. 22
IPS: Inline-Mode ............................................................................................................................................................ 23
Inside or Outside Sensor? ............................................................................................................................................... 24
Both – Network-Based IDS and IPS Deployment ......................................................................................................... 26
Notices ............................................................................................................................................................................. 27
Intrusion Detection Systems

Monitoring network traffic and/or host activity looking for

- Malicious traffic, such as attempts to circumvent identification &
  authorization or other access controls
- Reconnaissance traffic, such as port scans
- Unusual traffic: type, level, source, etc.

Then logging, reporting, and acting upon observed activity in a
prescribed manner

**087 Firewalls; the rules that we deal with
for them on most things are relatively
simple.

Intrusion detection systems are
looking for a particular type of
activity that has been studied in the
past and has been clearly labeled as
malicious.

That particular type of activity may
require a series of setup packets--
you know, like where we’d have to do
the three-way handshake first; and
then it-- of a certain way-- and then
it would pass it up through the stack,
where we’d look for well recombining
all of that stuff together and then
passing it up the stack; and we do that inspection inside the Intrusion Detection System.

The primary focus of Intrusion Detection Systems is not to stop packets; but it is to log and alert. That's its main job. So really it's an observer of the activity. That's different from an Intrusion Prevention System.

**IDS Characteristics**

May be signature or anomaly based

- **Signature**
  - Uses known pattern matching to signify attack

- **Anomaly**
  - Uses statistical variance or (sometimes) artificial intelligence (AI) engine to evaluate traffic, normal usage behaviors

The two main parts of an IDS are the sensor (or agent) and console

**088 Okay so what are the characteristics of an Intrusion Detection System? Well they can be signature based or anomaly based.**
This is relatively simple in its nature. There is a pattern of activity that has always bad. We've programed in the Intrusion Detection System rule that says: This is always bad, do not allow it through. That's one way.

The more sophisticated way is what's called anomaly-based. You know, I've been looking at this network for awhile; and this is the profile of this network and this is how it communicates.

You want to do what? That's anomalous to what the normal traffic patterns are back here; and so I'm going to reject that.

Now that could cause a problem. And we'll get to that in a bit.

Now there are two parts to an intrusion detection system: the center agent: the place where it's listening; and the actual console where a lot of the decisions are being made by the manager of this network.
Passive and Active Detection

Passive devices may log, monitor, and/or alert of intrusive activities, but do not take action to stop or block intrusion.

Active devices will take action based on the detected intrusive activity. Actions may include terminating processes, redirecting traffic, adding firewall rules to close ports, etc.

**089 There's also two different types. There's Passive and Active detection.

When we talk about Passive detection, all we're doing is logging all this activity; and we don't take any actions, there's no stopping whatsoever.

And then there's Active.

Here's the thing with an Intrusion Detection System. As this traffic—that traffic passed through, if it's an Active Intrusion Detection System, what it will do is it will send a reset.
If the evil was in the first packet and it gets through, and there's no reset to do-- and/or there's not reset to do- - then at that moment in time, well there's no reset to do; I can't really do anything. And if the evil gets through on the first packet, I really can't take any action.

So an Active Intrusion Detection System will actually take an action after the conditions are true; and not before.

**Detection Methods**

**Signature detection** relies on known attacks
- Will not be able to detect the “unknown”
- Example, detecting an exploit for a known vulnerability

**Anomaly detection** relies on finding “differences”
- Must first understand what is “normal”
- Example, detecting an exploit for an unreleased vulnerability
- Potential for false positives

**090 Now most of the time when we look at these detection mechanisms, and we talk about**
signature and anomaly-- remember that its signature is good; but it's not going to attack the- it's not going to be able to detect the unknown. It only looks for known vulnerabilities. So we have to have it. It won't do any good about zero-day attacks.

However the anomaly detection says: We're going to find the differences in the normal traffic pattern for these people back here; and we're going to say this is anomalous to that. And so a zero-day attack could be detected.

But here's the problem. Anything that is anomalous is going to be rejected; and that creates well business changes.

So therefore that creates a potential for false positives.
Detection and Inspection

Heuristic Scanning
- Differ based on technology
- Designed to detect the “unknown”, but not very successful
- Potential for false positives result in less sensitivity, thus less success

Bayesian Spam Filtering
- Statistical technique of spam filtering
- Correlates words with spam and non-spam e-mails then calculates probability that email is or is not spam

Packet Inspection
- Different IDS/IPSs and firewalls examine packets to different levels

Behavior Inspection
- Looks for variations in behavior, such as levels of traffic

**091 When we look at the detection and inspection-- how is this done; what do the brains of this thing actually look like? And so we have a bunch of different detection and inspection algorithms, if you will.

In Heuristic Scanning we look for-- they differ based on technology. Heuristic scanning is not as good as it should be at this moment in time. It is looking for something that it’s never seen before. It’s kind-- anomalous; but it’s statistical.

Now one of the other things that you could talk about is Bayesian Spam Filtering-- which is close to heuristics-
- to go ahead and say: This is-- I've never seen this before but this looks like spam; the tendencies, the statistics of this, that it doesn't actually fit with what I normally see as far as mail traffic is concerned. So I'm going to reject it. And Bayesian filters actually learn over time.

Packet inspection for IPS and IDS are—well they're just like firewall examinations; but they go to a different level.

They're looking for- instead of port or protocol- instead of port or IP address, now it's looking for if you scan inside the packet and you go deep inside of there and we see these two hexadecimal representations, along with these two hexadecimal representations, within this particular area; boy that's really deep down inside of what's going on.

So the Intrusion Detection Systems that are doing that packet inspection are deep down inside; and they have to be really quick and efficient.

And then there's Behavioral; which is a generic way to say that this is a variation in the behavior, such as a traffic level.

If we've got a mail server in the inside and it's used to a flow of 100,000 messages per day, and all of a sudden we start seeing more than 100,000-- you know, we get up about 150,000 messages a day or a million messages a day, some threshold in there-- that hey we're not going to allow that to go through.
Network-Based IDS (NIDS)

Connected to network segments to monitor, analyze, and respond to network traffic

Single sensor can monitor many hosts, requires management system for centralized monitoring

NIDS sensors are available in two formats

- **Appliance** – specialized hardware sensor and its dedicated software; use specialized NIC’s, processors, and hard disks to efficiently capture traffic and perform analysis.
  
  Examples: Cisco IDS 4200 series, IBM Real Secure Network

- **Software** – installed on server and placed in network to monitor network traffic

  Examples: Snort (most popular), Bro, Untangle

**092 Network Intrusion Detection Systems are- well they're sitting on the network itself. What we're doing is we're looking at a particular segment of traffic.

If I put a Network Intrusion Detection System at the edge of my network, it's going to see every single flow that there is. But if I take that same sensor and I put it way back inside, like next to the Accounting Department or at the chokepoint for the Accounting Department, it’s only going to inspect that traffic there.
So Network Intrusion Detection Systems are limited to the scope of what they can see.

Usually what we do is we-- we look at this in two different kinds of forms that are out there. One is appliance-based where you actually plug this thing in and turn it on; and the other version is software installation.

Now appliance-based has some software on it and it has to do updates. But it's a dedicated device. Whereas when we do the software, that's usually on an end-user's host system.

Now one of the examples that's listed here is Snort. Snort also comes with- you can also purchase it from the for-profit company that actually has it in a physical device itself that they ship along with it, that is special purpose optimized for that software.

And by the way, when we talk about Snort here; the open source community is still alive and supported and still working.
Network Intrusion Detection Systems (NIDS) – Characteristics

Network monitor

- Passively captures traffic and inspects it

Can also function in a client-server model

- Sensors are located on multiple machines across the network
- All sensors feed data to console
- Console machine handles logging and alerting

**093 When you look at network Intrusion Detection Systems characteristics, remember its job is to passively capture traffic and inspect it at a later time.

It can also work in a client-server model where we can have sensors located on multiple machines across the network; and we can aggregate all of that information. They can roll that up into a console; and it can be viewed and we can get a perspective on different pieces of the network.
NIDS – Advantages

Positioned properly, can test effectiveness of firewalls, router access lists, etc.

Can monitor multiple machines from one physical and logical location

Console can generate an alert if a monitored machine/network has ceased to send information

Operator can see patterns in traffic
  • Amount
  • Type

**094 The reason why we do Network Intrusion Detection Systems is because they don’t slow down the host. You can go at full speed; as long as this sensor or this tap can go ahead and pull the data off. And as long as the sensor can actually spin that stuff to disc, you can keep on going.

But remember, there is a size tradeoff here. And we're probably not going to be taking the entire packet and capturing it here. What we're going to be doing is is we're going to be looking for the packets that are bad and actually recording them; and the rest of the packets will...
drop away. Because we only have so much storage space.

And when you think about it, if we were to capture all the packet traffic that was coming into a network at that particular point, we’d have to have a hard drive or a list of an array of hard drives that was equal to all the hard drives that we’re trying to protect.

Now what happens is is the consoles that bring all this data together and aggregate all this data may be able to what we call “flip up.” We see suspicious traffic, and we’re only looking at the header information and only capturing the first number of bytes of the traffic.

Well if that goes wrong, then what we can do is we can say something’s not right there; now I want to turn on a new filter that captures all of the traffic including all of the data from that host to that host. So we can kind of upgrade what we’re capturing at that point in time.

Now remember the operator that’s getting all of this, can tune this; and they’re looking at this traffic going by. When are they there? I mean, this gets more under the business side of things. But are you willing to have somebody 24/7 sitting in front of the console?

A lot of people say: Well we don’t want to do that. So what we’ll do is we’ll-- and this dates me-- we’ll send a pager alert to the person who is
supposed to be there so that they can go ahead and take their precious time off and give it back to the company for reviewing this particular communication.

It turns out with all the false positives, a lot of- well a lot of frustrated security administrators would chuck their pager out the window of their car as they're driving down the road.

And now we do it through text messaging. But what we find is is all that communication could, unless it's tuned correctly, could drown the security administrator and make them run to the office over and over and over again.

Remember, the Network Intrusion Detection Systems can see patterns in traffic over a long period of time, if you're collecting that data over a long period of time.

And it also looks at the type.
NIDS – Disadvantages

Since it is capturing all network packets, can produce large log / alert files

- Can be difficult to cull through vast amount of information

Console machine generally must be quite powerful, similar to a workgroup server

If console machine goes down then multiple machines may be left unmonitored

Communication from sensors to console may increase overall network traffic levels

**095 Okay there's some bad stuff here.

Since the packet capturing is all the network packets, it can produce those huge log files. So that's our first problem. And so we can get all the good stuff and all the bad stuff, all the trash that's going in there.

Now that console that's rolling all this stuff up and doing an analyzation on it, really has to work very, very hard. So if this machine goes down, or multiple machines-- if this machine goes down, this console, then all of those well devices that it's protecting are now unprotected. So we probably need to have some redundancy in there.
Now when we get to communication from the sensor to the console, unless we’ve got a separate segment just dedicated to that, we could overwhelm that particular host.

**NIDS – Typical Deployment Environments**

**NIDS – Typical Deployment Environments**

Generally seen in a corporate or organizational environment

- Multiple assets to protect
- Maintain personnel levels

Inside / outside protected network to monitor firewall effectiveness, public hosts (DMZ)

**096 Let’s look at some typical deployments. We're going to look at this as multiple asset protection and multiple personnel protection, both inside and outside the DMZ and see how it works for us.**
Intrusion Detection/Prevention System

**Intrusion Detection System (IDS)**
- Passive monitoring for attacks
- Monitoring and responding to alerts
- Potential for false positives

**Intrusion Prevention System (IPS)**
- Active blocking of attacks
- Potential for false positives

**097 Before we do that, we need to talk about crossing over from intrusion detection to intrusion prevention.**

In intrusion detection, we passively monitor all that information. We log it; we may alert at a console,

In Intrusion Preventions Systems what we say is: We know this is definitely bad traffic. So what we're going to do is we're going to block those active attacks. We're literally going to say: None shall pass; like the Dark Knight.

There's a potential for false positives there; and those false positives-- now
since we’re rejecting traffic completely, this could cripple the business or the mission that’s actually occurring.

**IDS: Promiscuous-Mode**

**IDS: Promiscuous-Mode**

A network device sends copies of packets to the sensor for analysis.

If the traffic matches a signature, the sensor sends an alarm to a management console and a response action can be taken.

**098 So first we talk about the IDS in Promiscuous Mode saying: A network device is going to send an extra copy of the traffic.**

Notice in this diagram here we have a router at the edge, a switch in between the two different routers; and we’re spanning-- it’s called span port-- we’re pulling a copy of those and sending them to a sensor.
That sensor is going to examine that traffic; and then it’s going to roll metadata back up to the management system. It’s not going to actually put the packets there. It’s going to put metadata there.

So it’s going to match the particular signature on the sensor; and then it may take a corrective action going back.

When I look at this diagram what I see is if this sensor was able to pass true traffic back to this management system, we have two different ways to get to this network.

We have to make sure that only metadata is rolling back here to this particular host. That’s the thing that we have to be careful about.

I have seen configurations where this is actually now connected to another network, or it’s connected to the yellow network if you will, so that there are two paths for the data to flow. And if we can overcome the switch with whatever traffic and we can overcome the sensor, then what we’ll do is we’ll use this sensor as a launching point to attack this management console, and then use this management console to attack a particular target on the inside.

So you want to be careful about how you configure this. Only the metadata should flow. I think that those management consoles should not be attached in any way, shape or form to the local area network or what we’ll call the production network.
**IPS: Inline-Mode**

The sensor resides in the data forwarding path.

If a packet triggers a signature, it can be dropped before it reaches its target.

An alert can be sent to the management console.

**099 Now we could do this inline.**
What we could is we moved--
And here let’s go back for a second.
IDS: Promiscuous-Mode

A network device sends copies of packets to the sensor for analysis.

If the traffic matches a signature, the sensor sends an alarm to a management console and a response action can be taken.

**098 We could take this sensor and push it up there.**
**099 And then post the traffic down here. That means that this host on the management system—this management system is now potentially attackable as another host on this network, as another target on this network.

Again I think that this should be isolated away. I would even take the management console and put it up here and put it into its own special network. I would not use VLANing for it. I would actually use physical connections to it.

Now the problem is when using physical connections-- there’s only so
long this wire can be between these things; and that could cause problems as far as cost is concerned.

So the sensor can reside in that data forwarding path. But then it’s now susceptible to the evil that’s going on out there; especially if it’s detected.

**Inside or Outside Sensor?**

**Inside or Outside Sensor?**

<table>
<thead>
<tr>
<th>Sensor on Outside</th>
<th>Sensor on Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sees all traffic destined for your network</td>
<td>• Sees only traffic permitted by firewall</td>
</tr>
<tr>
<td>• Has high probability of false positives</td>
<td>• Has lower probability of false positives</td>
</tr>
<tr>
<td>• Does not detect internal attacks</td>
<td>• Requires immediate response to alarms</td>
</tr>
</tbody>
</table>

**Attacker**

**Internet**

**Inside**

**100** So where should my intrusion detection sensor be? Should it be on the inside of my network? Should it be on the outside of my network? Should it be close to the cloud and close to the attacker? Or should it be behind some sort of filtering device?
I don't know what the answer is for your organization. I see sensors on the outside and sensors on the inside.

What I find is really interesting is that there are some organizations that will actually do both; and they'll actually compare the two. And then what they're saying is: Is this device filtering properly between these two networks? That requires a lot of extra work.

So remember that the sensor on the outside sees all the network traffic; and has lots and lots of false positives. And it doesn't have any visibility on the inside.

The sensor on the inside sees only traffic permitted by the firewall; that filters. And if the firewall is doing its job that's good. Less false positives; and really it requires immediate response by personnel.
**101 We could do both an Intrusion Detection System and an Intrusion Prevention System.

Intrusion Prevention Systems-- in this case when we put them up here before we got to our- after we've gotten through our traffic, what we can say is: We've filtered a lot of stuff here. But anything that gets back here as far as the Intrusion Prevention System is concerned, we'll take the chance of false positives back there. It's worth our chance because what we want to do is protect these clients from whatever evil is out there.
And then what we can also do is we can put an intrusion detection sensor here, within our shared services or our DMZ, to look at what’s going on with these hosts here. Because there’s so much traffic flowing back and forth here, all we can do is log and alert; and then take care of it later on and hope that our firewall going into our local area network is protecting us.