Intrusion Detection / Prevention Systems

IDS / IPS

07th September 2021

Network Security and Performance Workshop - UPROUSE with LEARN

Thilina Pathirana

Based on and Credits: APNIC, APRICOT, NSRC, SANOG Security Tracks

Intrusion Detection

There could be an intruder even if you have security practice in place

To detect these loop holes, Security practitioners recommend IDS to be deployed as a network service which act as another layer of monitoring to confirm the Security.

IDS Capabilities

- Detect successful attacks
- Look for various things that shouldn't be there
- Infected files
- Look for potential attacks on other machines
- Packets that shouldn't exist
- Strange patterns of behavior
- Contain attacks before they spread further
- Recognition of pattern reflecting known attacks
- Statistical analysis for abnormal activities

What they Can't do

- Compensate for weak authentication & identification mechanisms
- Investigate attacks without human intervention
- Guess the content of your organization security policy
- Read encrypted data
- Compensate for weakness in networking protocols, for example IP Spoofing

What we see - - ALERTS

- You may receive tons of millions of alerts
  - –Depending on your detection rules
  - –There are many suspicious activities in the Internet today
- You should notice a critical one at least
  - –Detection rule is important!

If your rules are not tuned,

- False Positive / Type I Error:
  - –is the incorrect rejection of a true null hypothesis
  - –is when a system raises an incorrect alert
- False Negative / Type II Error:
  - –is the failure to reject a false null hypothesis
  - –is when an attack pass undetected

Types of Detection

- Signature Based
  - –Match patterns against known attacks
  - –Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities
- Anomaly Based
  - –Look for unusual behavior
  - –Detect any action that significantly deviates from the normal behavior

Detection vs Prevention

An IPS (Intrusion Prevention System) executes real-time responses to active attacks and violations. An IPS is the same as an IDS but with Active Defense. System administrators should structure rules within the IPS unique to their needs. This allows not only for monitoring and evaluation of threats but also for real time action to stop an immediate threat. An IPS is an active defense that can catch intruders that might go unnoticed by firewalls or anti-virus software.

Using an IDS or IPS depends on you need and your tolerance for false positives blocking valid traffic.

Institutes desiring an extensive view into their networks would benefit from an IDS.
Those who wanting immediate automatic action taken against internal and external attacks would benefit from setting up an IPS.

Which one should you deploy

If implementing your own system, take care when choosing between the various IDS/IPS vendors. Different vendors have a myriad of options and details about their product you need to assess against your needs.

The two most important factors are:

NETWORK SPEED: How much traffic can the IDS / IPS process?

UPDATES: How frequent are their updates for signatures and rules, and do they cost extra?

Open Source IPS/IDS Snort

- Snort is an open source IDS, and one of the oldest ones with hundreds of thousands of users
- Active development of rules by the community make Snort up to date, and often more so than commercial alternatives
- Snort is fast! It can run at Gbit/s rates with the right hardware and proper tuning
- You could run Snort in multiple ways

  –As a device “in line” behind or after the firewall/router

  But this adds one more element that can fail in your connectivity

  –Or you could use a span/mirror port to send traffic to Snort (recommended)

Update Snort Rules

- The commercially maintained snort rules are available for free with a 30 day trial
- Other rules are maintained by some volunteers at emerging threats: http://rules.emergingthreats.net/open/
- But not all rules will make sense in your network
- You will want to customize which rules you want to run
- Otherwise you will get many false positives, which will lead you to ignore Snort, or simply turn it off...
- It doesn't help to have logs full of junk alerts you don't want
- To avoid this, rules can be suppressed (disabled)

Snort Rules

alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg: "SSH Detected"; sid:10; rev:1;)

The text up to the first parenthesis is the **Rule Header** and the section enclosed in parenthesis contains the **Rule Options**.

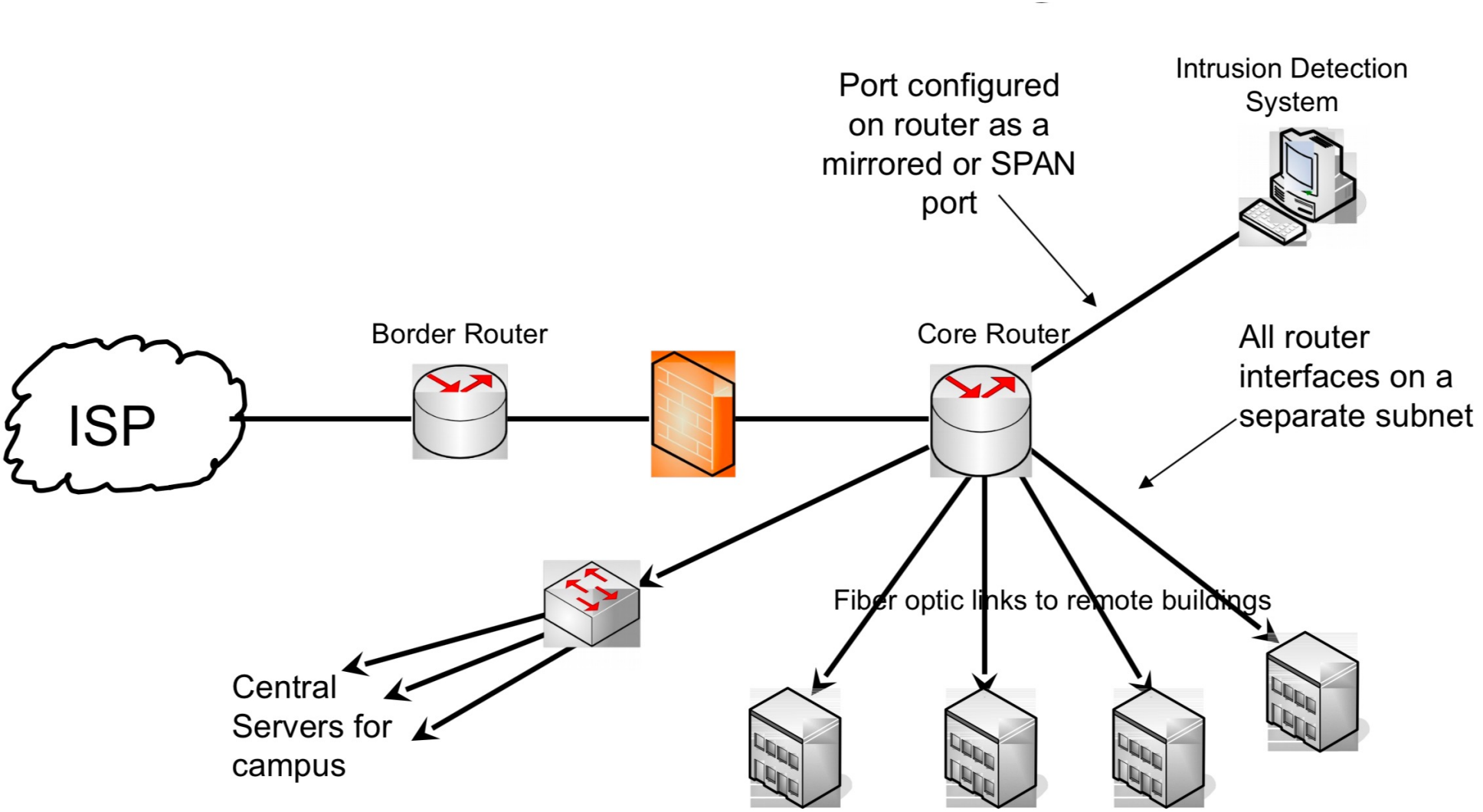
The words before the colons in the rule options section are called option keywords.

- The sid keyword is used to add a “Snort ID” to rules
  - –Range 0-99 is reserved for future use
  - –Range 100-1,000,000 is reserved for rules that come with Snort
  - –All numbers above 1,000,000 can be used for local rules

IPS Installation with pfsense

Source: NSRC

Traditional Network Setup



Source: NSRC

Traditional Network Setup

Any device you put in-line with all your traffic can become a bottleneck

You may only have 10M today, but soon it will be 100M, then 1G, then 10G

Traffic filtering / inspection / shaping at higher rates is extremely expensive

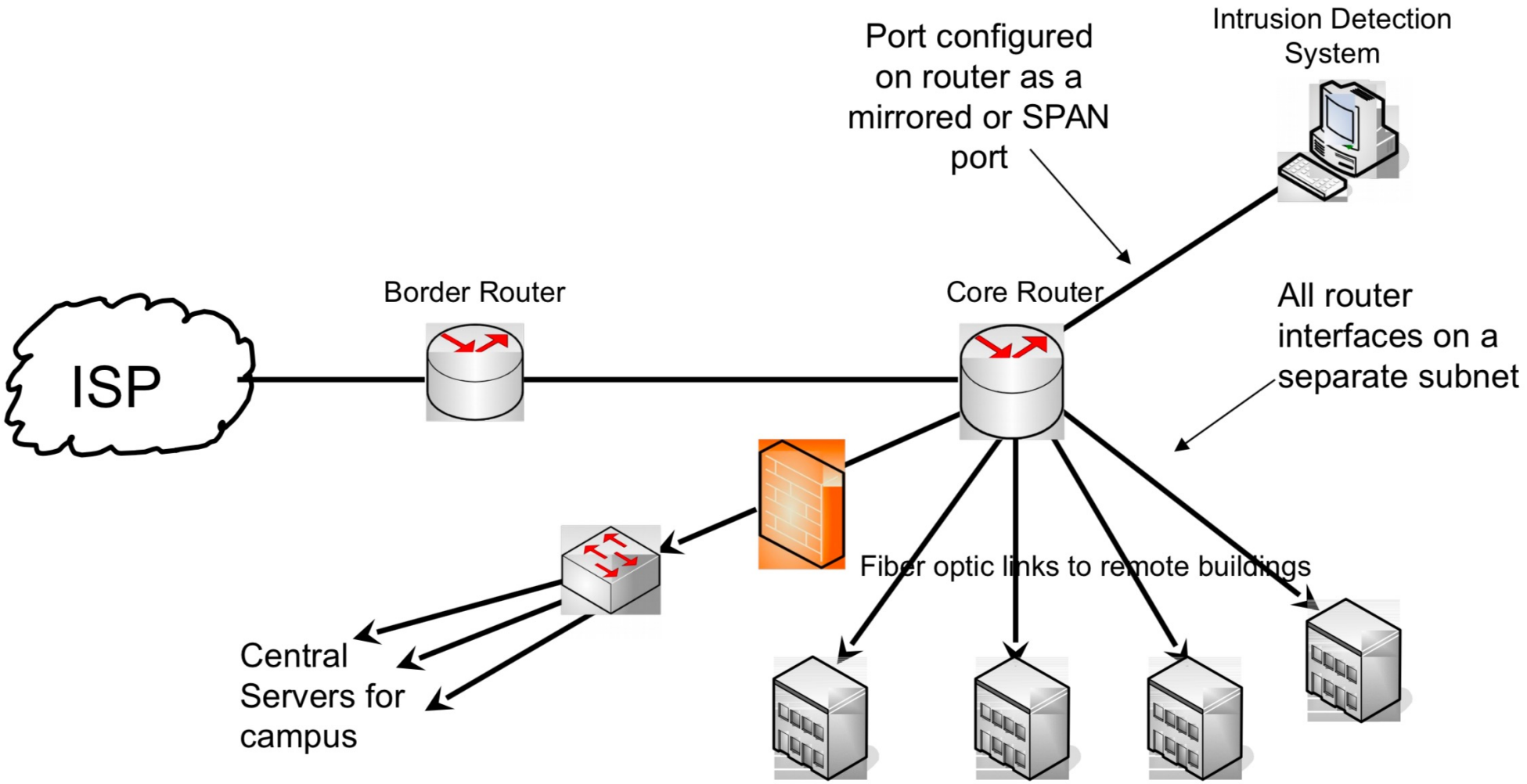
Search for “science DMZ” – many sites now bypassing firewall entirely

All desktop machines have built-in firewalls that protect them from being attacked from the network

Firewalls limit performance and cause bottlenecks.
– Firewalls should only protect critical assets

– This allows firewalls to more tightly protect the critical assets even from attacks from “inside”

New Approach



Source: NSRC

100% Secure Systems

Our defenses aren't perfect

- Patches weren't applied promptly enough
- Antivirus/ IDS/ IPS signatures not up to date
- 0-days get through
- Someone brings in an infected USB drive
- An insider misbehaves

Now what?

Most penetrations are never detected, allowing continuing abuse, and helps the attackers spread elsewhere.

Nothing is 100% secure.

Thank You

Thilina Pathirana