



# Agenda

1. Progression of Packet Filtering
2. Intrusion Detection and Analysis
3. Concepts of IDS and IPS
4. Use Cases for IDS and IPS
5. Attacks and Countermeasures
6. Vendor Technologies
7. Additional Resources

# 1. Progression of Packet Filtering

- Firewalls
- Stateful inspection
- Deep packet inspection
- UTM or Next Gen firewalls
- Application layer firewalls
- IPS and signature based filtering

## 2. Intrusion Detection and Analysis

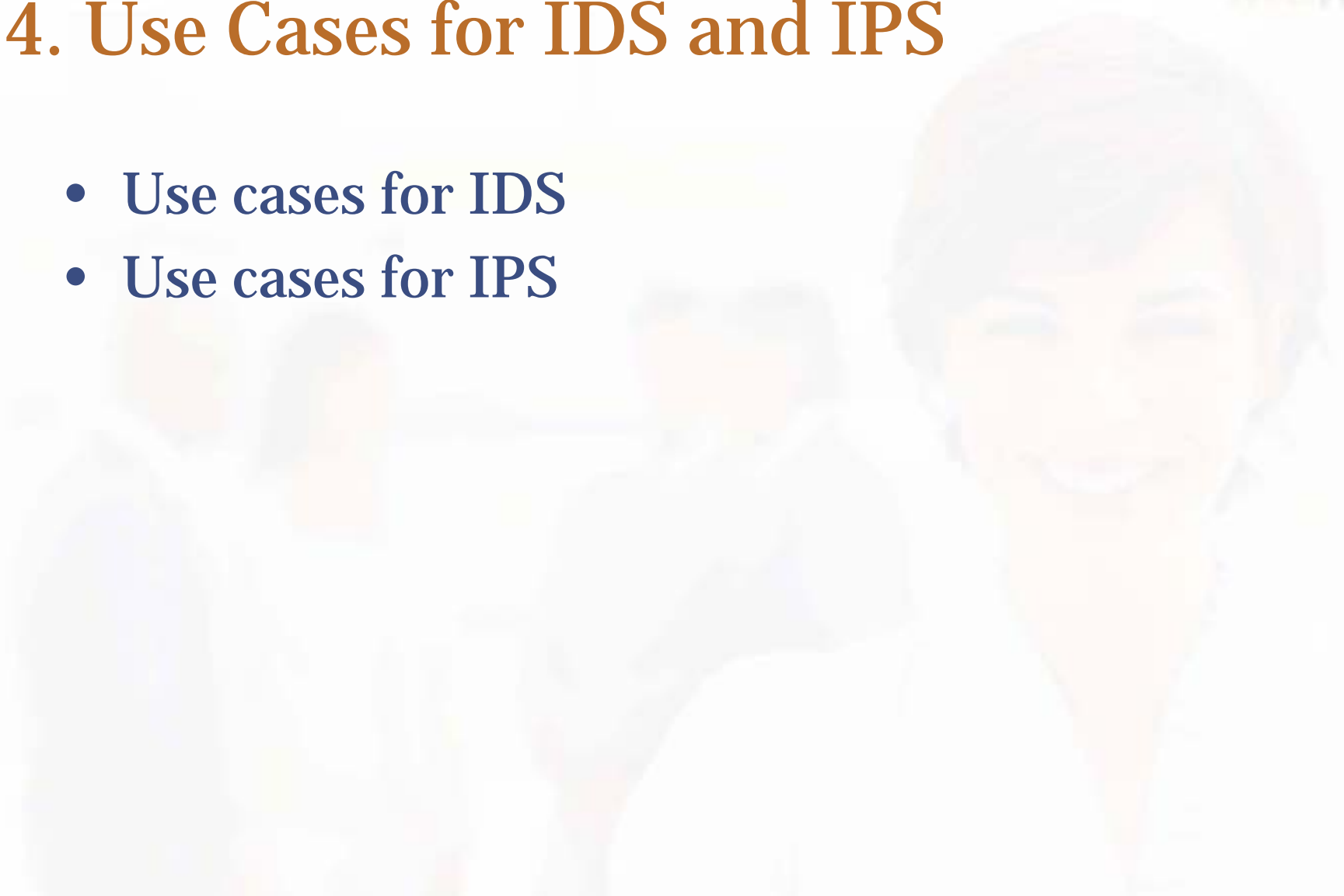
- Protocol analysis
  - Examples
    - TCPdump
    - Wireshark
- Flow analysis
  - sFlow
  - NetFlow
  - JFlow
- Network Behavior Anomaly Detection (NBAD)
- IDS/IPS

## 3. Concepts of IDS and IPS

- Concepts of IDS and IPS
  - All About the Hosts
- Host based vs Network based
- Use of Protocol Analysis in IDS and IPS
- Detection methods of IDS and IPS
  - Behavior based
  - Signature based
- IPS as enforcement and correction

## 4. Use Cases for IDS and IPS

- Use cases for IDS
- Use cases for IPS



## 5. Attacks and Countermeasures

- Insertion
- Evasion
- Denial of Service
- Protocol Attacks
- Application Attacks
- Attacking IDS versus IPS Systems

## 6. Vendor Technologies

- IBM
- McAfee
- Cisco
- Juniper
- Sourcefire IPS
- Snort
- 3<sup>rd</sup> Party Evaluation

< Vendor details not included in public slide set >

## 7. Additional Resources

- Links coming



# Thank You!

**Jennifer Jabbusch**

**CISO, Network Security Specialist**

**Carolina Advanced Digital, Inc.**

[www.cadinc.com](http://www.cadinc.com)

[jj@cadinc.com](mailto:jj@cadinc.com)

**Security Blogger**

[www.SecurityUncorked.com](http://www.SecurityUncorked.com)

