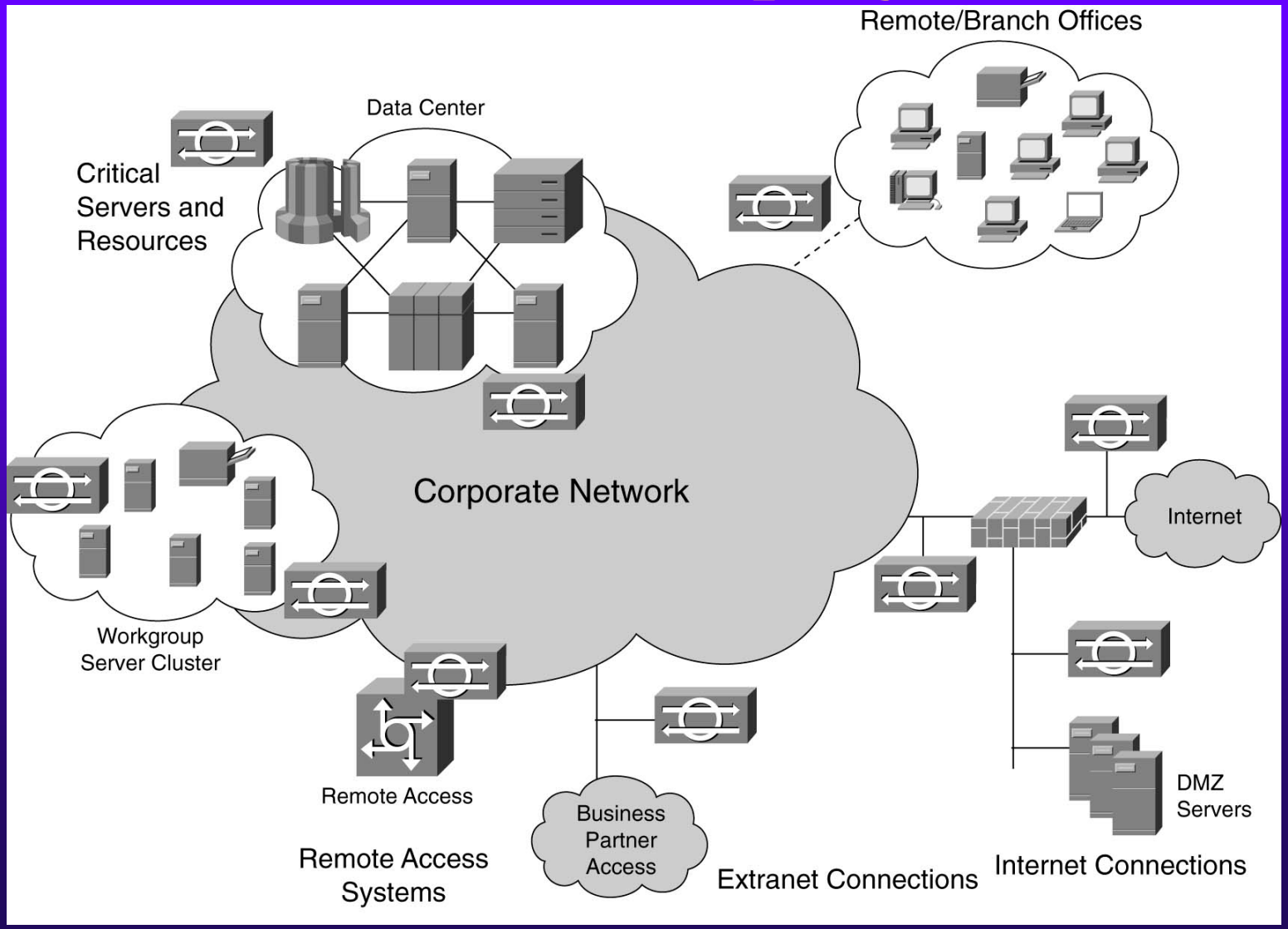
Chapter 15

Cisco Secure Intrusion Detection

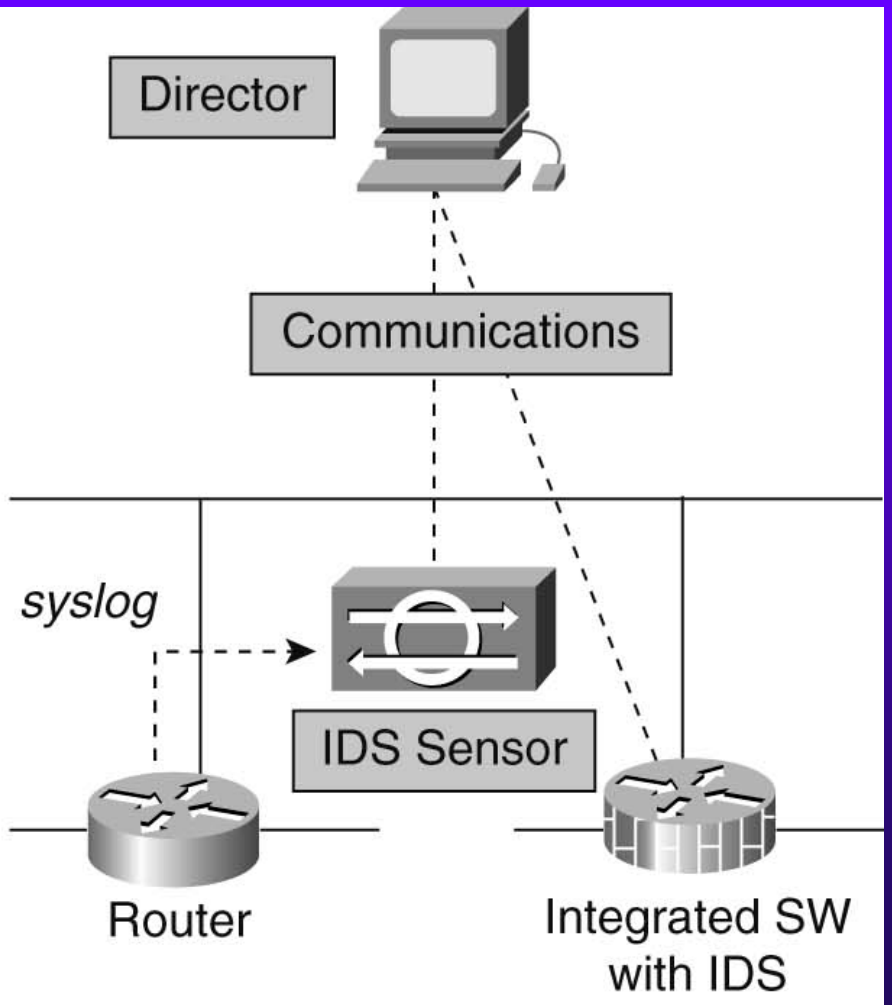
Location of IDS Sensor Deployment



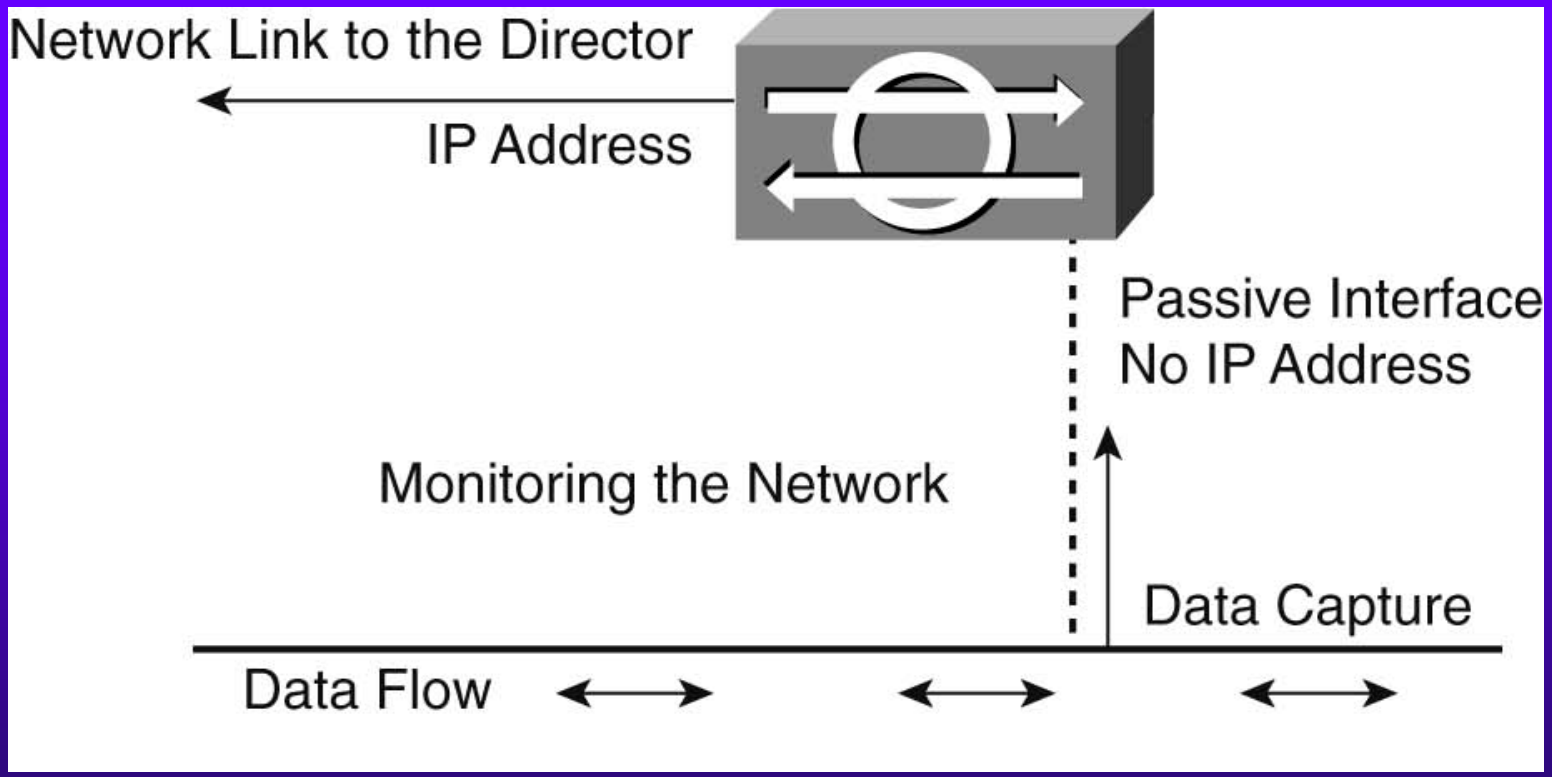
Interaction between IDS Sensor and Management Console

Director
- Real-time Alarm Display
- Appliance Configuration
- Signature Distribution

Sensor
- Packet Signature Analysis
- Generate Alarms
- Response/Countermeasures



IDS Sensor


Network Link to the Director
IP Address
Passive Interface
No IP Address
Monitoring the Network
Data Capture
Data Flow

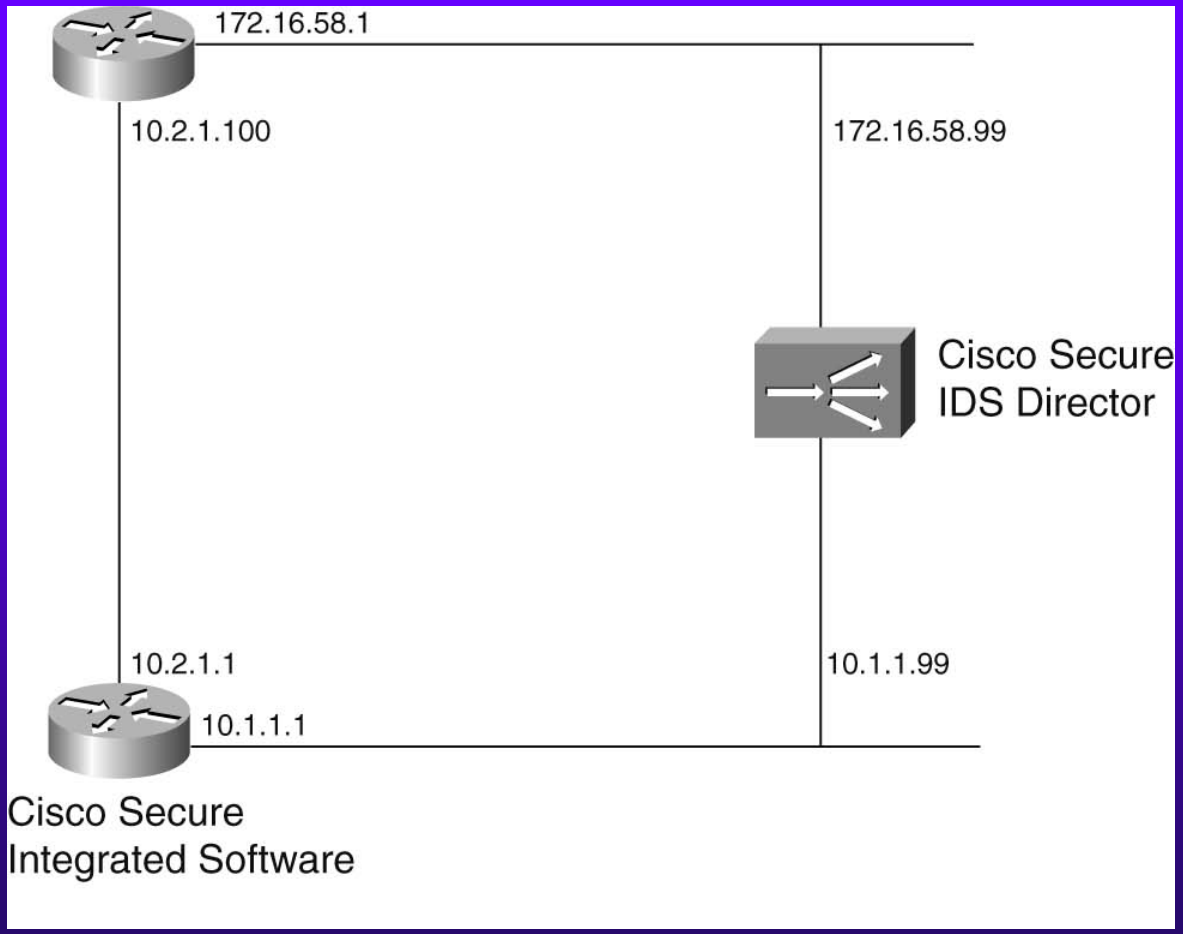
Sensor Response to Intrusions

- No action
- Shun
  - Block attack by creating ACLs dynamically
- Log
- TCP Reset

IDS Signatures

- Signatures supported by Cisco IDS appliances and IDSM (1000+)
  - http://www.cisco.com/cgi-bin/front.x/csec/idsAllList.pl
- Signatures supported by IDS software in Cisco IOS router (< 100)
  - http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm#xtocid127

Using a Router as the IDS Sensor



Note: Cisco Secure IDS Director has been replaced by CiscoWorks VPN/Security Management Solution (CWVMS)