Planning for Incident Response

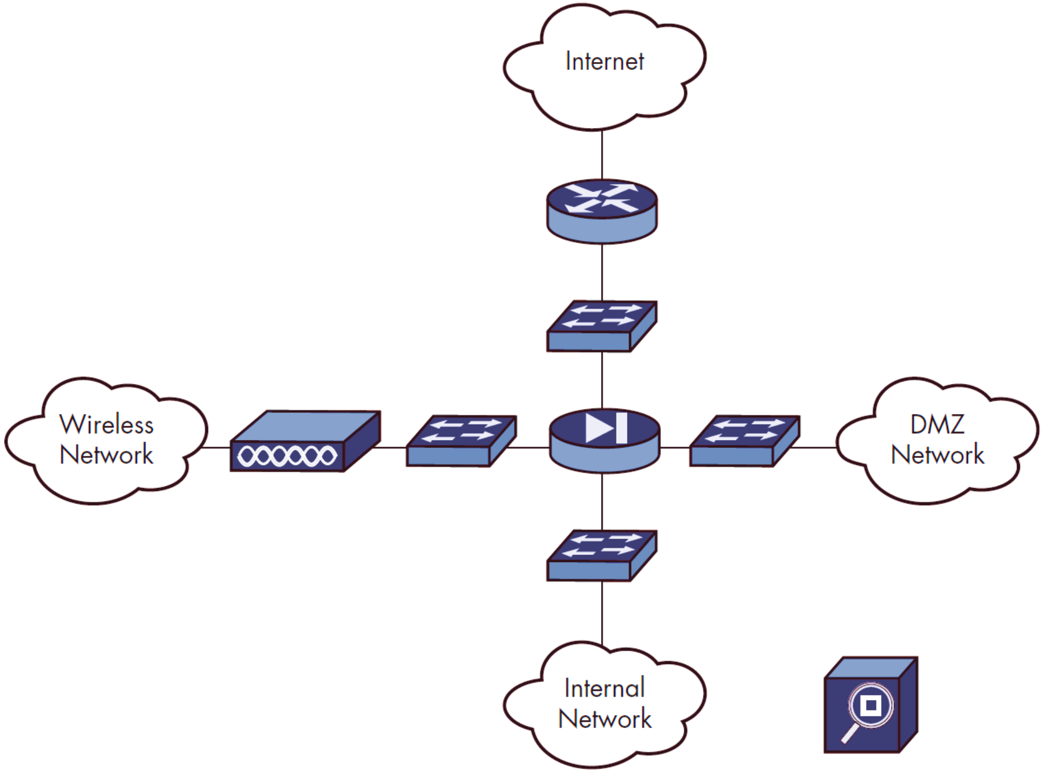
INFO-6081 – Monitoring & Incident Response

FANSHAWE

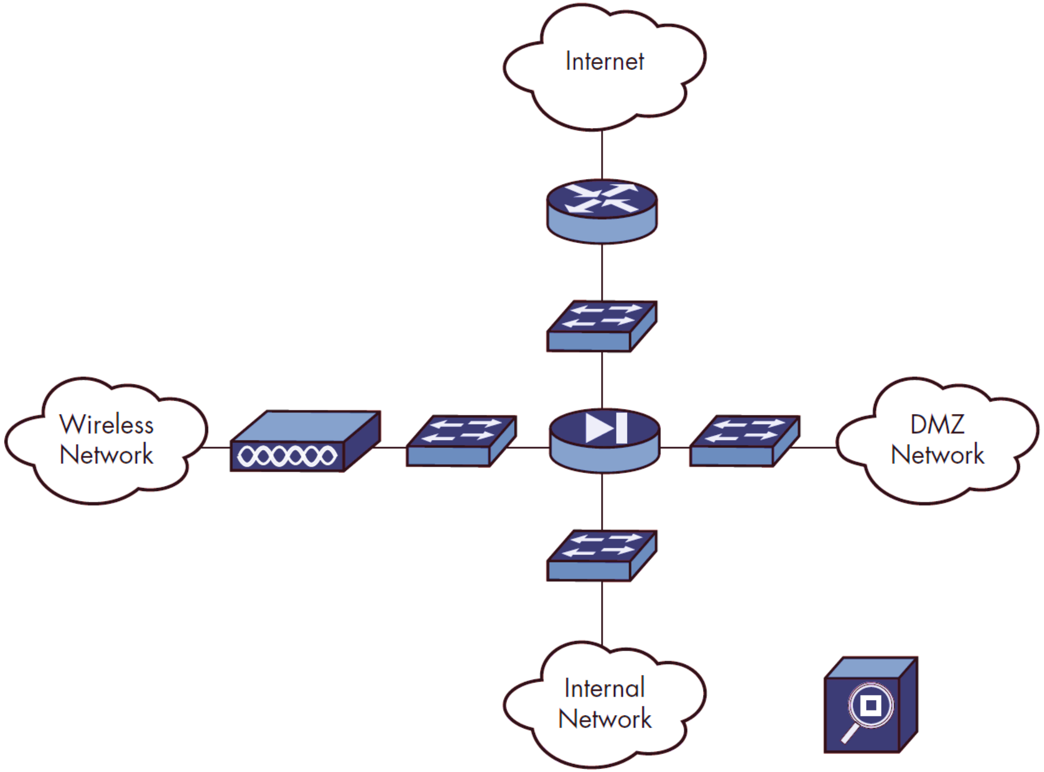
Learning Outcomes

- Sensor Placement
- NSM Sensor Hardware Requirements
- NSM Platform Management Recommendations
- Incident Response Planning
- Forming the IR Planning Team
- Developing the Incident Response Policy
- Planning the Response
- Training & Testing
- Assembling and Maintaining the IR Plan

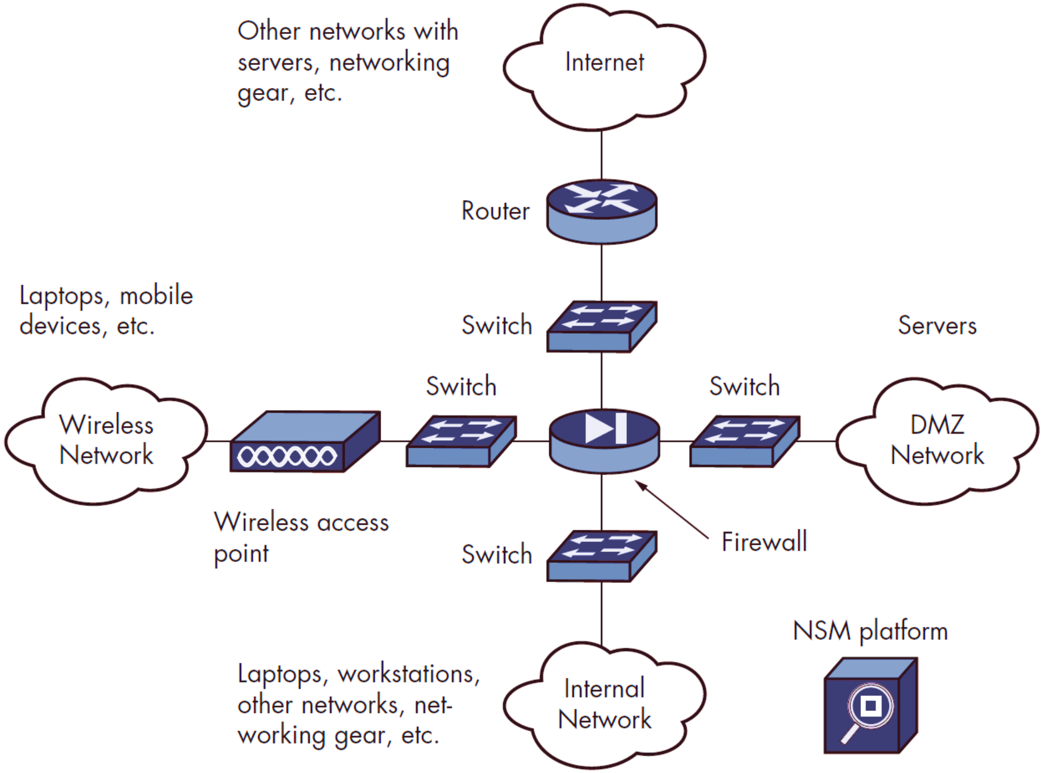
Sensor Placement



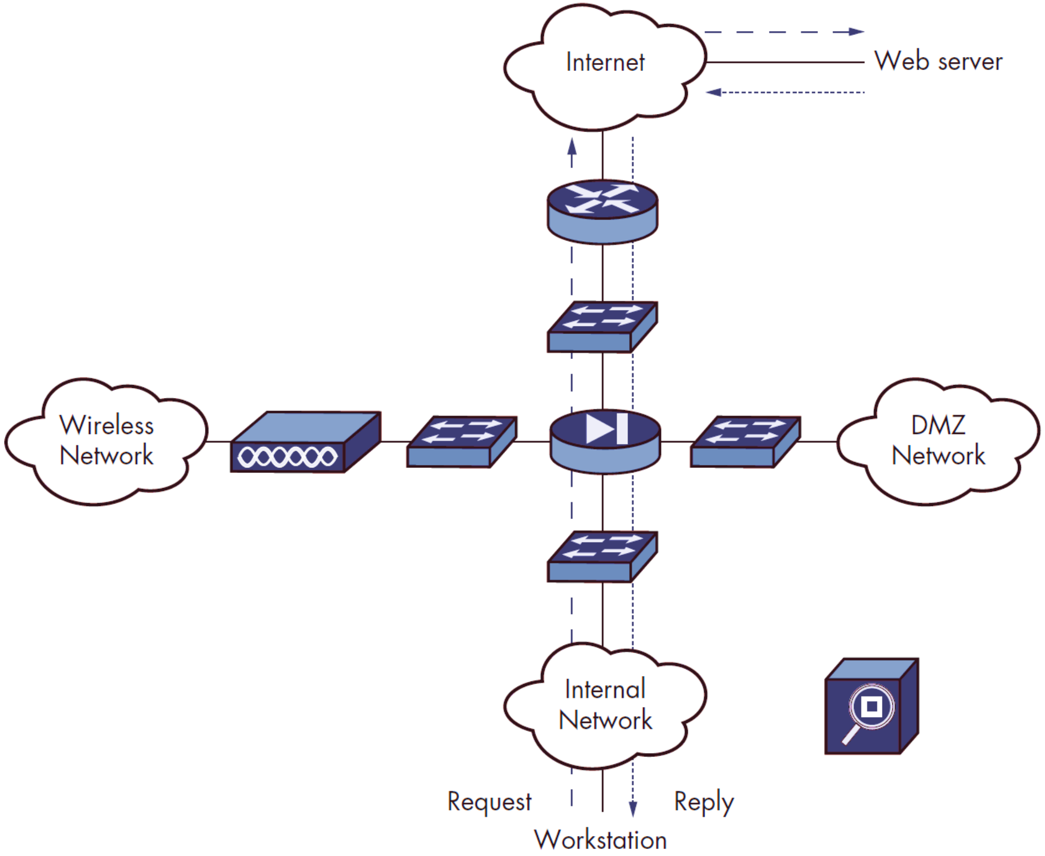
Sensor Placement



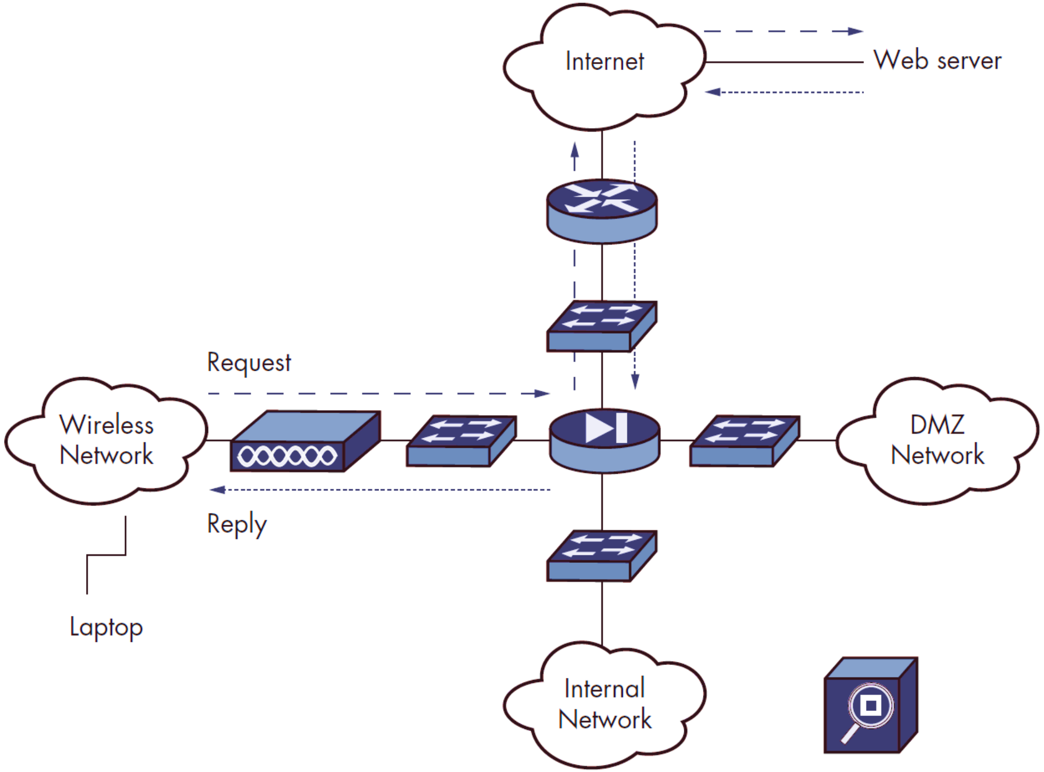
Sensor Placement – Devices


Other networks with servers, networking gear, etc.
Internet
Router
Laptops, mobile devices, etc.
Switch
Servers
Switch
Switch
Wireless Network
DMZ Network
Wireless access point
Switch
Firewall
NSM platform
Laptops, workstations, other networks, net-working gear, etc.
Internal Network

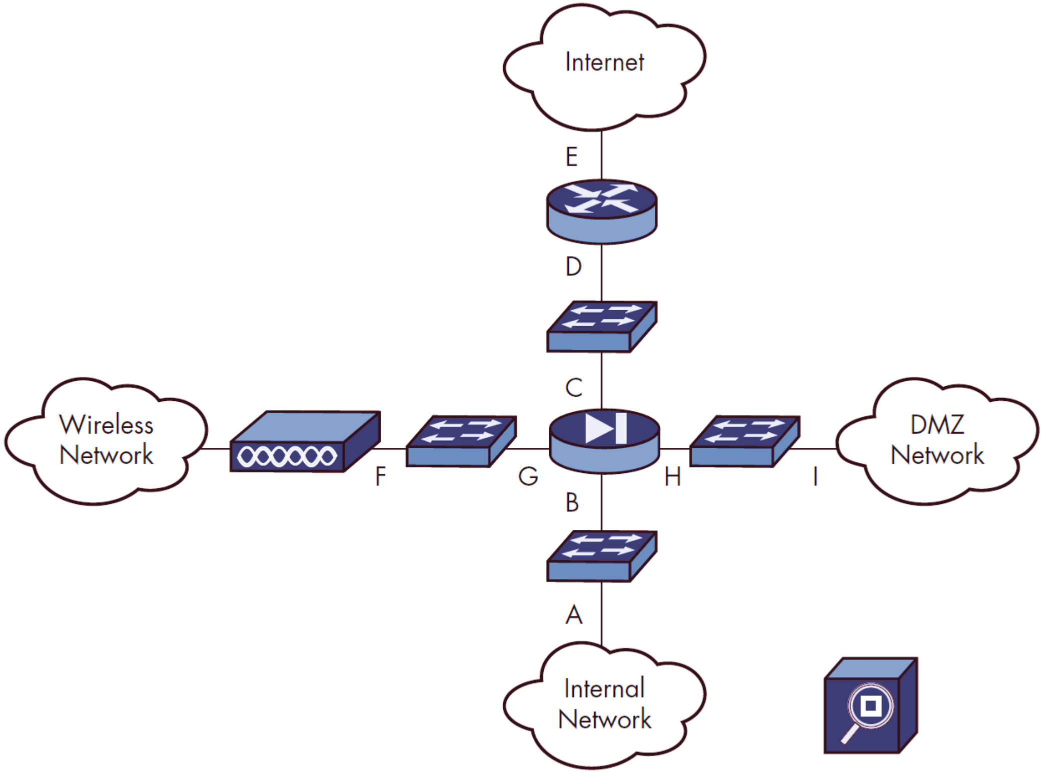
Sensor Placement – Traffic Flows



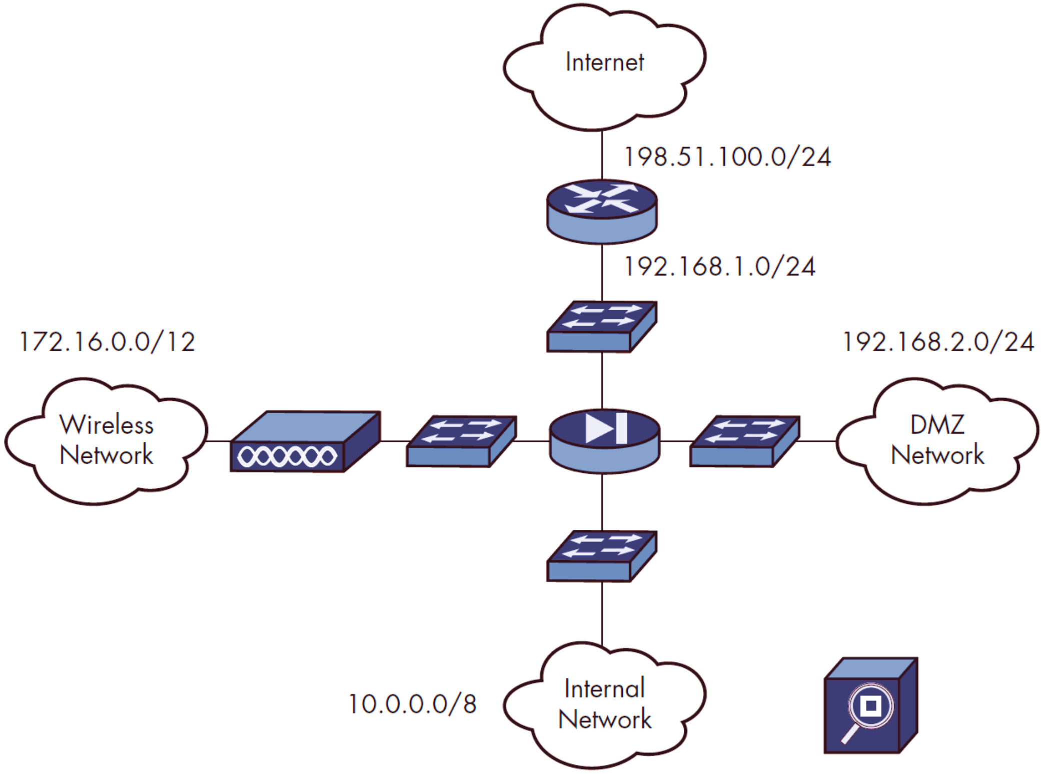
Sensor Placement – Traffic Flows



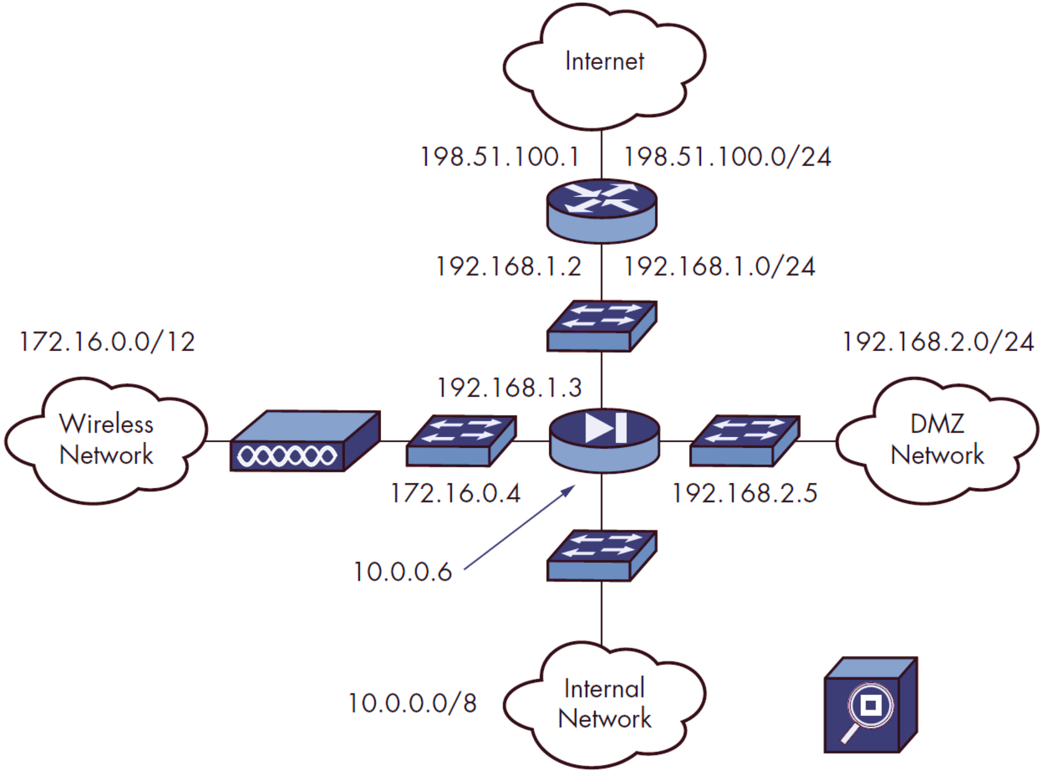
Sensor Placement – Possible Locations



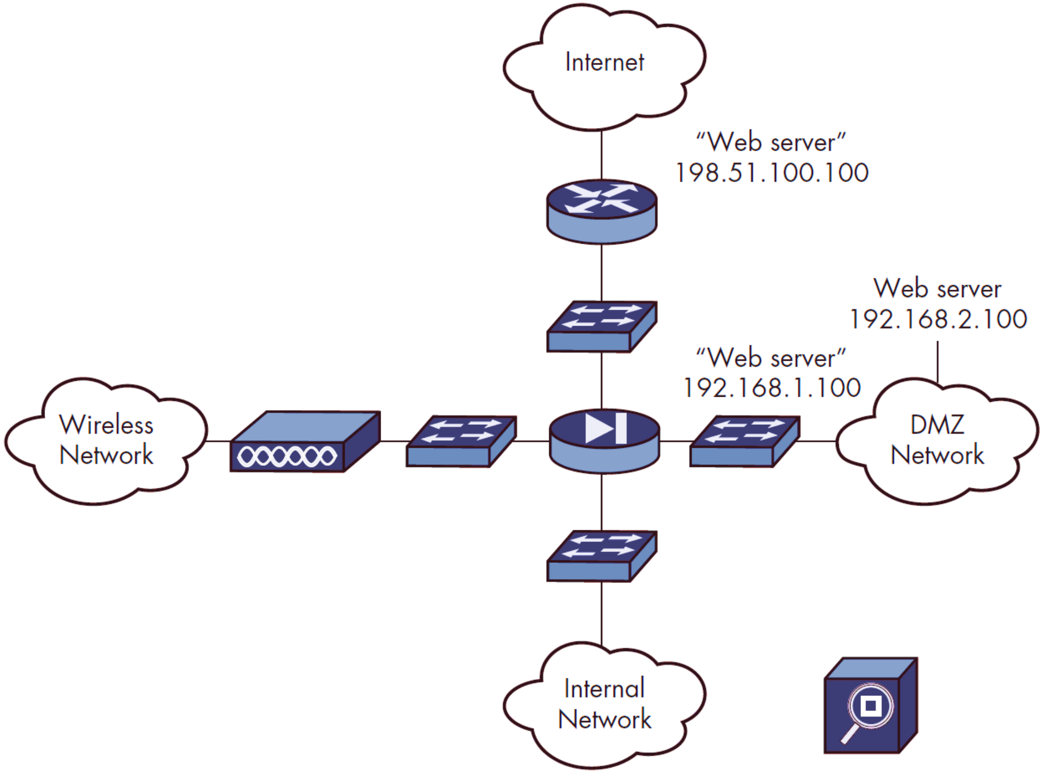
Sensor Placement – Network Addressing



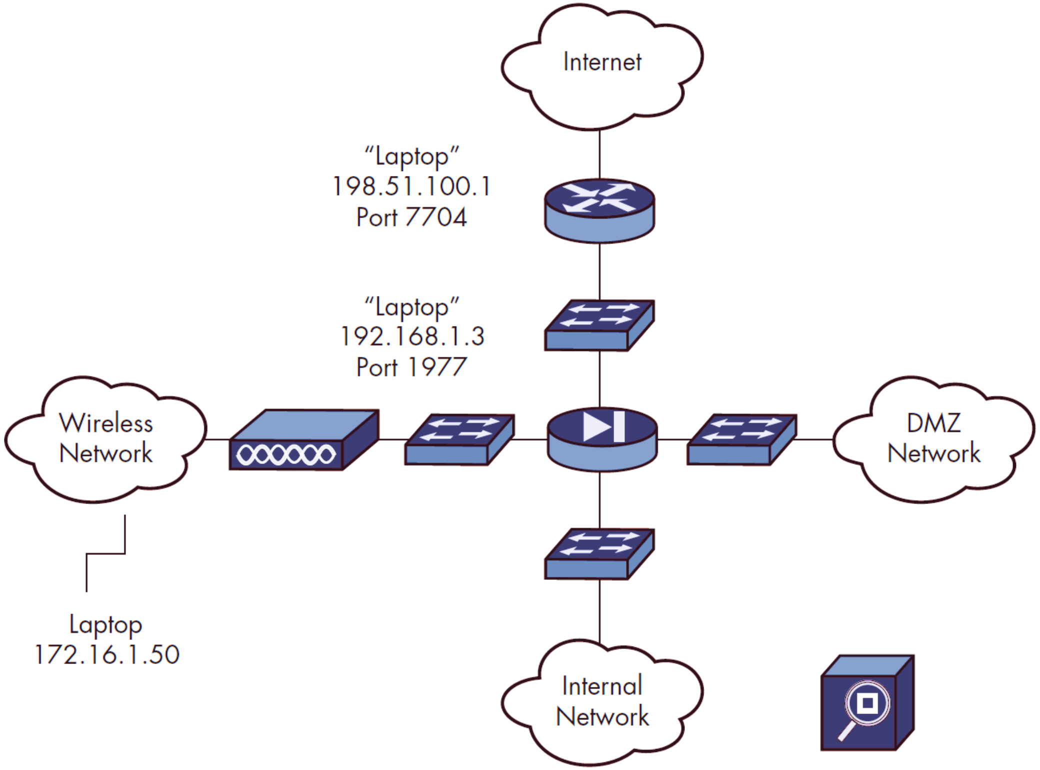
Sensor Placement – Interface Addressing



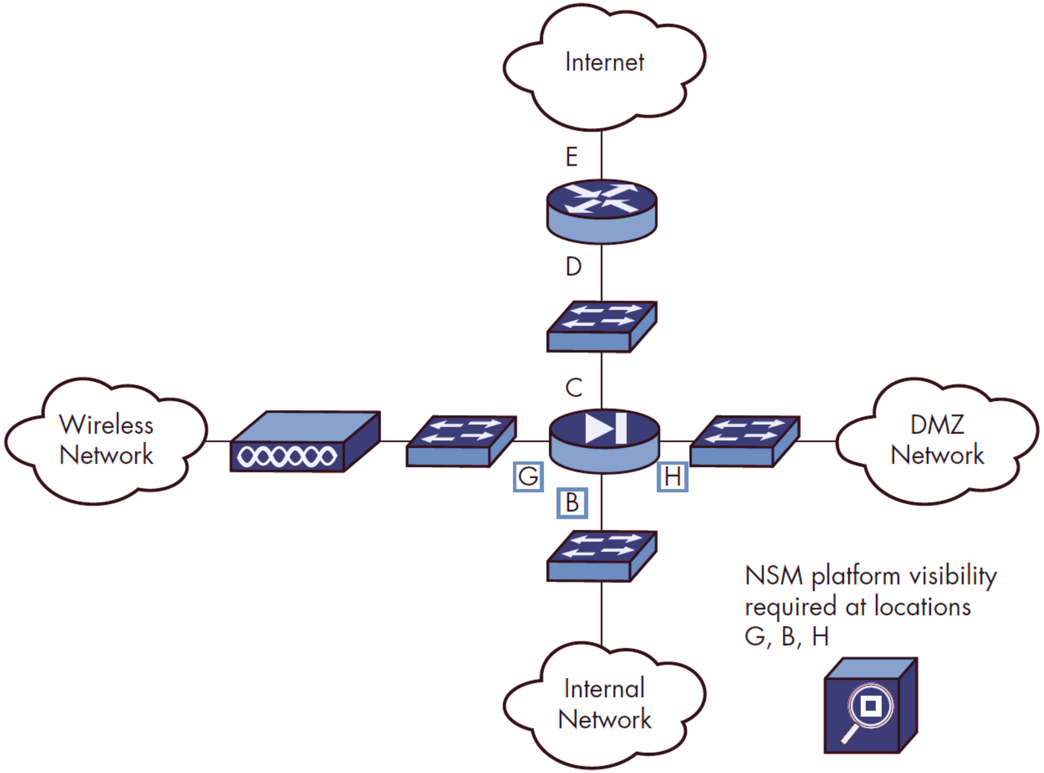
Sensor Placement – Network Address Translation



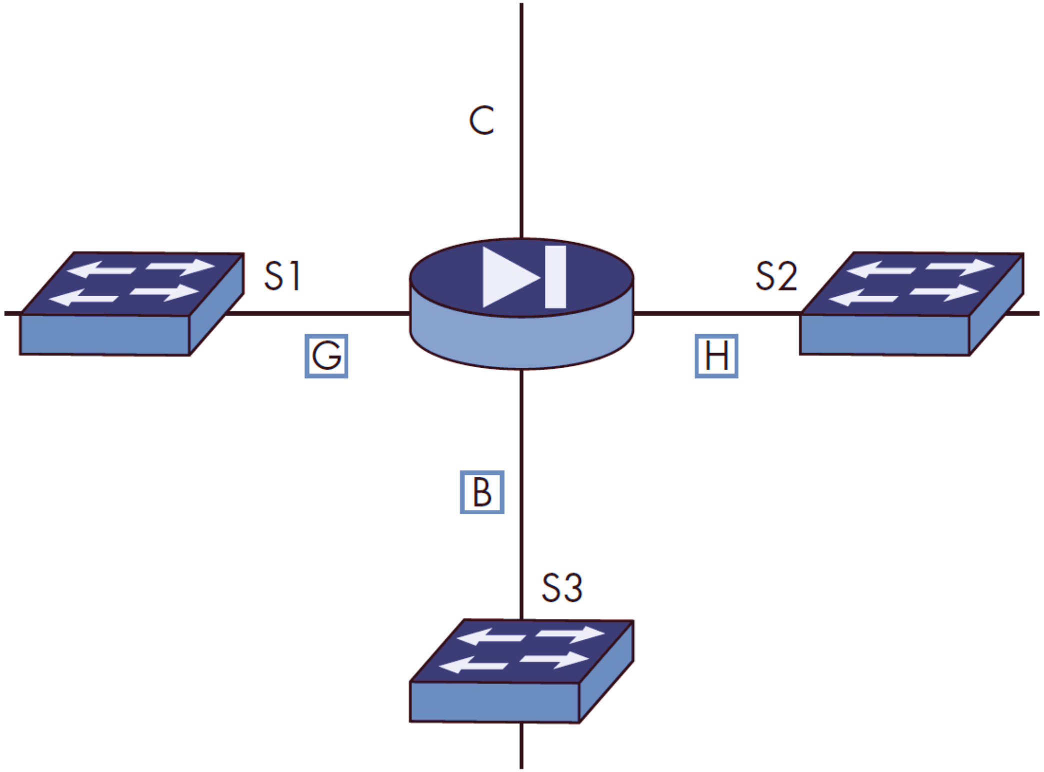
Sensor Placement – Port Address Translation



Sensor Placement – Traffic Visibility



Sensor Placement – Port Mirroring



SPAN Ports vs Taps

SPAN Ports

- No additional hardware required
- Configurations can be adjusted easily

- Easy to oversubscribe
- Requires ports normally used for devices

Taps

- Most continue to operate even after a power failure
- Less likely an intruder can modify the configuration

- Adds additional expense when purchasing equipment

NSM Sensor Minimum Hardware Requirements

- Processor: 8 Core x86-64 CPU
- Memory (RAM): 8-128 GB
- Hard Drive: A large array of RAID 10 (preferred) storage, based on monitoring requirements
- Network connection (LAN) : At least 2, 1 for management and another for traffic capturing

Storing Full Content Data

- Hard drive storage for one day = Average network utilization in Mbps × 1 byte/8 bits × 60 seconds/minute x 60 minutes/hour × 24 hours/day

Example:

- **100**Mbps × 1 byte**/8** bits **× 60** seconds/minute **× 60** minutes/hour **× 24** hours/day **= 1,080,000**MB per day or 1.08TB per day

- 12.5MB per second, 750MB per minute, 45GB per hour

NSM Platform Management Recommendations

1. Limit shell access to only the administrators that need it
   - Analysts should only log in directly in an emergency
   - They should regularly use the remote access tools provided
2. Administrators should never use the root account
   - The only reason to use the root account is to enter single-user mode if the sensor is unable to boot
   - Logon sessions should be protected with multi-factor authentication
3. Always use secure remote administration methods
4. Do not centralize the sensor's user accounts with AD

NSM Platform Management Recommendations

5. Equip production sensors with a remote-access card
6. Limit the exposure of the sensor, and keep services up-to-date
7. Employ remote logging services for sensor logs
8. Connect the management interface to a network segment dedicated for management activities
9. Use full disk encryption to protect data when powered down
10. Include the sensor in the regular software update schedule

Incident Response Planning

FANSHAWE

Contingency Planning

- Contingency Planning includes all activities carried out by an organization to prepare for the unexpected
- The Incident Response (IR) process focuses on detecting, analyzing, and reacting to an incident, the later phases of the process focusing on keeping the organizations resources running
- Whenever possible, the IR process should contain and resolve incidents
- If the IR process cannot contain and resolve an incident, the organization turns to the Business Resumption (BR) plan to help resume normal operations

Contingency Planning

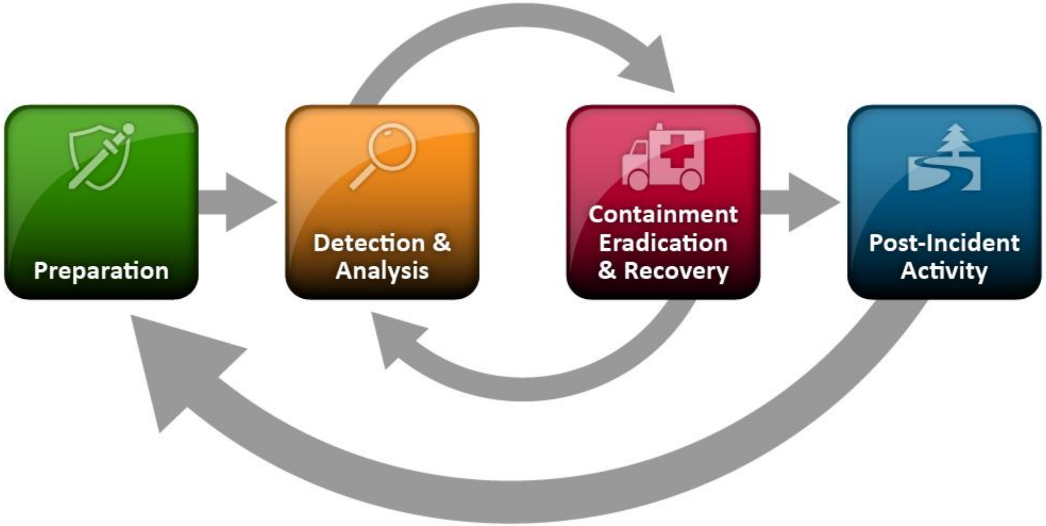
- The overall IR process is made up of several phases: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity

Incident Response Planning Process

- As an output from the business impact analysis (BIA), the IR committee, disaster recovery (DR) committee and the business continuity (BC) committee each receive information on potential attacks they may face
- In the case of incident planning, the group follows these general stages:
  - Form the IR planning committee
  - Develop the IR planning policy
  - Integrate the BIA
  - Identify preventive controls

Incident Response Planning Process

- Organize the CSIRT
- Create IR strategies and procedures
- Develop the IR plan
- Ensure plan testing, training, and exercises
- Ensure plan maintenance



Forming the IR Planning Team

- With the assistance of communities of stakeholders that will be affected by the IR process, the executive management will build the team that is responsible for all subsequent IR planning and development activities
- The Incident Response Planning team (IRP team), should consist of individuals from relevant constituent communities, most notably the CSIRT
- As a result, the IRP team will typically have strong representation from the IT and Information Security teams

Forming the IR Planning Team

- The IRP team will work to build the IR policy, plan and procedures that the CSIRT will follow during the IR actions
- Similar to other organizational teams, the IRP team will require a champion, ideally the chief information officer (CIO) or the vice president of IT
- The group should meet regularly, first to develop the IR policy, then to complete development of the IR plan
- The IRP team is also responsible for the structuring, development, and training of the CSIRT at the appropriate juncture in the planning process

Developing the Incident Response Policy

- With the support and input of the group that built the IRP team, one of the first deliverables is the IR policy
- The policy should define the operation of the team, articulate the organizational response to various types of incidents, and advise end users on how to contribute to the effective response of the organization
- Just as the enterprise information security policy defines the roles and responsibilities for information security for the entire organization, the IR policy defines the roles and responsibilities for IR

Developing the Incident Response Policy

The components of a typical IR policy include:

- **Statement of management commitment**
- **Purpose and objectives of the policy**
- **Scope of the policy**
- **Definition of information security incidents and their consequences within the context of the organization**
- **Organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the IR team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting types of incidents**
- **Prioritization or severity ratings of incidents**
- **Performance measures**
- **Reporting and contact forms**

Developing the Incident Response Policy

- The IR policy must gain the full support of the top management and be clearly understood by all affected parties
- It is also of vital importance to gain support of the communities that will be required to alter business practices or make changes to their IT infrastructure
  - If the CSIRT determines the only way to stop a massive denial of service attack is to sever the organizations connection to the internet, it should have a signed document preauthorizing such action

Developing the Incident Response Policy

- As with developing other policies, the involvement of those who will use the policies is critical in their development
- Involving related CP teams (DR and BC) will aid in the development of clear, consistent and uniform policy elements across the organization

Incident Response Planning

- An incident response plan (IR plan) is a documented set of processes and procedures that anticipate, detect and mitigate the effects resulting from an IT security incident or breach
- According to contingency planning an adverse event that threaten the organization's information is called an incident
- An incident occurs when the adverse event affects information resources causing actual damage or disruption
- The IR plan is activated when an incident causes minimal damage with little to no disruption to business operations

Incident Response Planning

- Events causing damage beyond this would typically be classified as disasters
- With the aid of any communities of interest, the creation of an IR plan typically falls to the chief information security officer (CISO) in conjunction with the IRP team
- The roles and responsibilities of the IRP team and the CSIRT should be clearly document and communicated
- The IR plan should also include an alert roster that lists critical agencies to be contacted during an incident

Incident Response Planning

- The IRP team should seek to develop a series of predefined responses that will guide the team and information security staff through the IR steps
- Having predefined responses allows an organization to improve response times without confusion or added effort

Incident Response Planning

- For every potential attack scenario, the IR team creates an incident plan, which includes three sets of incident handling procedures, the steps to be take during, after and before an incident:
  - **During the Incident**
    - Addresses procedures that must be performed
    - These procedures are grouped and assigned to individuals, with tasks appropriate to job function
  - **After the Incident**
    - The procedures that must be performed immediately after the incident has ceased

Incident Response Planning

- **Before the Incident**
  - The tasks that must be performed to prepare for an incident
  - These include details of backup schedules, DR preparation, training schedules, testing plans, copies of service agreements, BC plans, etc.
  - This section of the plan is only a priority when incident response is not underway
- The IRP team will add other information such as a trigger, notification details and response times, which can vary based on the priority of the incident

Planning the Response

- Contrary to most planning methods, incident response begins with the actions that are immediately necessary after an intrusion has been detected (during the incident)

Triggering the IR Plan

  - Each attack scenario is examined and a “trigger” is determined
  - The trigger describes the circumstances that cause the IR team to be activated and the IR plan to be initiated
  - Some examples of triggers include:
    - Notification from the helpdesk or system administrators about unusual behavior

Planning the Response

  - Notification from an IDS device
  - Unusual patterns found in system or network logs
  - Failure of the network, or individual components
- It is the responsibility of the IR duty officer to determine if the IR plan should be activated and to contact the appropriate reaction force as defined by the IR plan
- As the skills required to mitigate various security threats vary, the IR plan should list the personnel required to best respond to the intrusion
- Documentation is a key component of every network, and a scribe should be appointed to document the incident

Planning the Response

Actions required “During the Incident”

- Next, the actions required to react to the incident are planned
- If the organization is experiencing a malware infestation, the first step is to verify it’s existence on a system
- Communication is a key component of the response, and the helpdesk is a go to point of contact for users; therefore, the helpdesk should be instructed about potential signs that the infestation has spread
- Once the infestation has been confirmed, the reach of the compromised systems must be assessed

Planning the Response

- Next, efforts should shift to quarantine the affected systems to prevent further damage
- Once all affected systems have been quarantined, the boundary of quarantine must be confirmed
- The team should also be looking for flare ups
- When all affected systems have been isolated, decontamination can begin

Planning the Response

Actions required "After the incident"

- When the incident has been contained, lost or damage data must be restored
- The IR plan should outline the steps required to recover from the incident
- It should also describe actions required such as protection to avoid follow-up incidents, forensic analysis and after-action review
- The after-action review is a detailed examination of the events that occurred, from the initial detection to the final recovery
- All team members review their actions during the incident, reviewing what worked, what didn't, and what should be changed for future actions

Planning the Response

Actions required “Before the incident”

- Actions required before an incident include the best practice IT and information security techniques practiced by most IT departments; however, some incidents may have unique characteristics that require additional measures
- Prevention and preparation methods are also included as before actions such as rehearsal, training and testing of the IR plan

Training the CSIRT

- A primary responsibility of the IRP team is to train the CSIRT to be ready for potential incidents
- Training can take the form of IR plan rehearsals, internal on-the-job instruction, or completion of courses held by external training entities or vendors
- In addition to this, the organization should provide developmental assistance to less experienced employees
- One of the most important components of training the CSIRT is to test the IR plan

Testing the IR Plan

"Give me six hours to chop down a tree and I will spend the first four sharpening the axe."

- unknown

- Few IR plans are executable as initially written, and must be tested to identify faults and overlooked actions
- Regular tests provide insight into how smoothly the CSIRT will respond during an actual event
- Once problems have been identified, changes to the process can be documented and implemented

Testing the IR Plan

- Some strategies used to test the IR plan:

  Desk Check

  - Distribute copies of the plan for review by all team members that will have actions to take

  Structured Walk-Through

  - Team members gather in a conference room to discuss the actions that would occur at every step of the process

  Simulation

  - Each member of the team simulates the performance of each task
  - No physical actions are taken

Testing the IR Plan

Parallel Testing

- Team members act as if a real incident is happening and perform the required tasks, without interrupting the production environment, or affecting business operations

Full Interruption

- A full test of the plan, that includes any tasks that may result in an interruption of service
- During a full interruption, restoration of backup data is performed

War gaming

- A simulation of attack and defense strategies using realistic systems
- The CSIRT should be acting as defenders and testing the procedures outlined in the IR plan

Training the Users

- In addition to training the CSIRT, the end users require training to assist in the IR process
- Training the end users is normally performed as part of the security education training and awareness program (SETA)
- User training should address the following areas:
  - What is expected of them
  - How to recognize an attack
  - How to report a potential incident
  - How to minimize the damage an attack can cause
  - Information security best practices
  - Identifying social engineering attacks
  - Correct procedures for acquiring new software
  - How to handle password and other sensitive information

Assembling and Maintaining the IR Plan

- A draft plan can be used to training and testing to evaluate the effectiveness of the plan
- Any errors or omissions should be remedied and the version of the plan incremented
- When the desired level of maturity is attained, the final assembly can commence
- Once the “final” plan is assembled, it should be tested semiannually with the team performing at least a structured walkthrough, with more detailed testing performed as often as possible

Assembling and Maintaining the IR Plan

- Any areas of the plan that are changed as a result of after-action review, should be scheduled for re-testing at the earliest opportunity
- Every organization will have preferences for the format and content of the plan, but the following recommended practices make it easy to locate in an emergency:
  - Keep the plan in a brightly coloured binder (red or yellow)
  - Place reflective tape on the spine of the binder
  - Place a classified document cover sheet as the first page
  - Place an index on the first inside page, preferably with colour-coded tabs

Assembling and Maintaining the IR Plan

- Place each category of attack, place the corresponding IR plan document under a common tab and label the index
- Organize the contents in the order: during the incident, after the incident, before the incident
- Insert copies of any relevant documents in back of the binder (service agreements)
- Add any other related documents
- Store in a secure, but accessible location

Summary

- When deploying network sensors, it is important to consider the visibility of network traffic, as well as the hardware used for monitoring
- Full Content Data places high demand on storage systems
- Incident Response is a component of contingency planning, and aims to contain and eradicate incidents before they turn into disasters
- The IRP team will work to build the IR policy, plan and procedures that the CSIRT will follow during the IR actions
- The IR plan is activated when an incident causes minimal damage with little to no disruption to business operations

Summary

- An incident plan includes three sets of incident handling procedures, the steps to be take during, after and before an incident
- Two critical components of the IR planning process is the training of personnel and testing the IR plan

References

- Bejtlich, R. (2013). Chapter 2: Collecting Network Traffic: Access, Storage, and Management. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.
- Security Onion Solutions. (2020). Security Onion: Security Onion Documentation. Evans, GA: Author.
- Whitman, M. E., Mattord, H. J., & Green, A. (2014). Chapter 4: Incident Response: Planning. Principles of incident response and disaster recovery (2nd ed.). Australia: Course Technology Cengage Learning.

References

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. doi: 10.6028/nist.sp.800-61r2