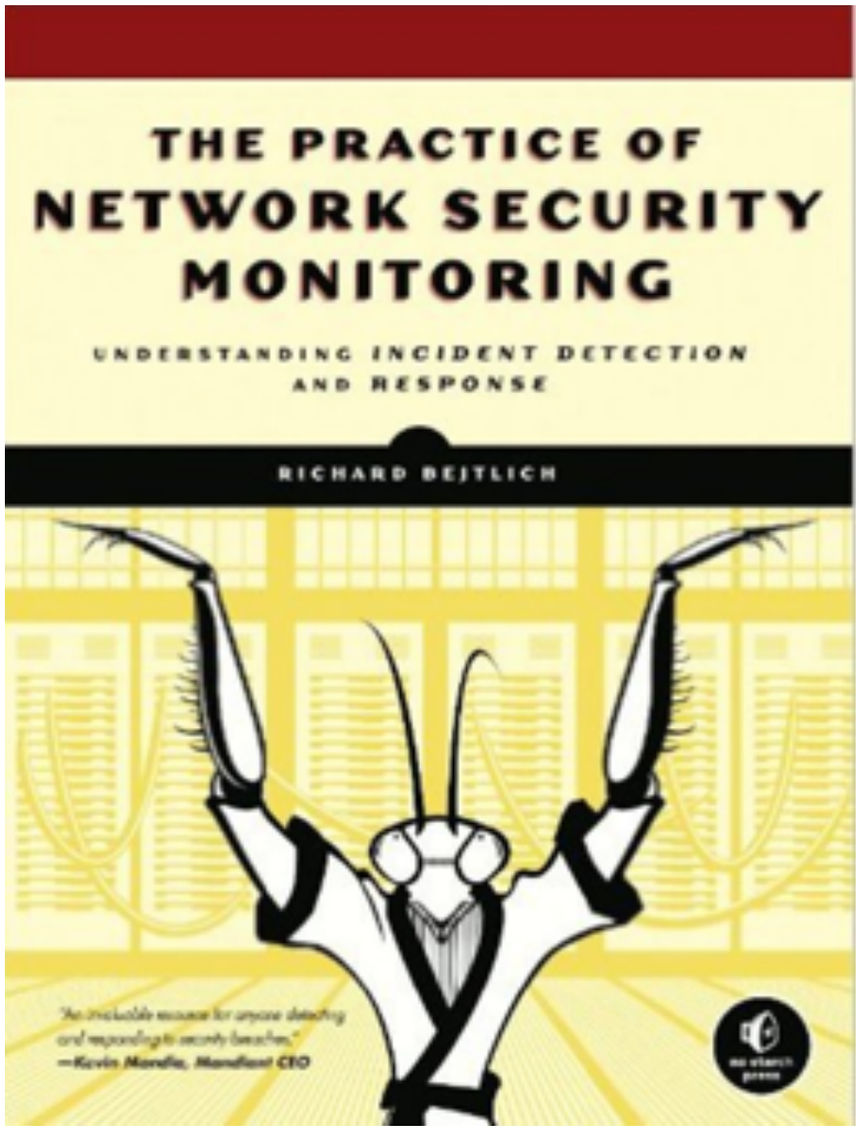
CNIT 50:
Network Security Monitoring

2. Collecting Network Traffic: Access, Storage, and Management



Topics

- **A Sample Network for a Pilot NSM System**
- **IP Addresses and Network Address Translation**
- **Choosing the Best Place to Obtain Network Visibility**
- **Getting Physical Access to the Traffic**
- **Choosing an NSM Platform**
- **Ten NSM Platform Management Recommendations**

A Sample Network for a Pilot NSM System

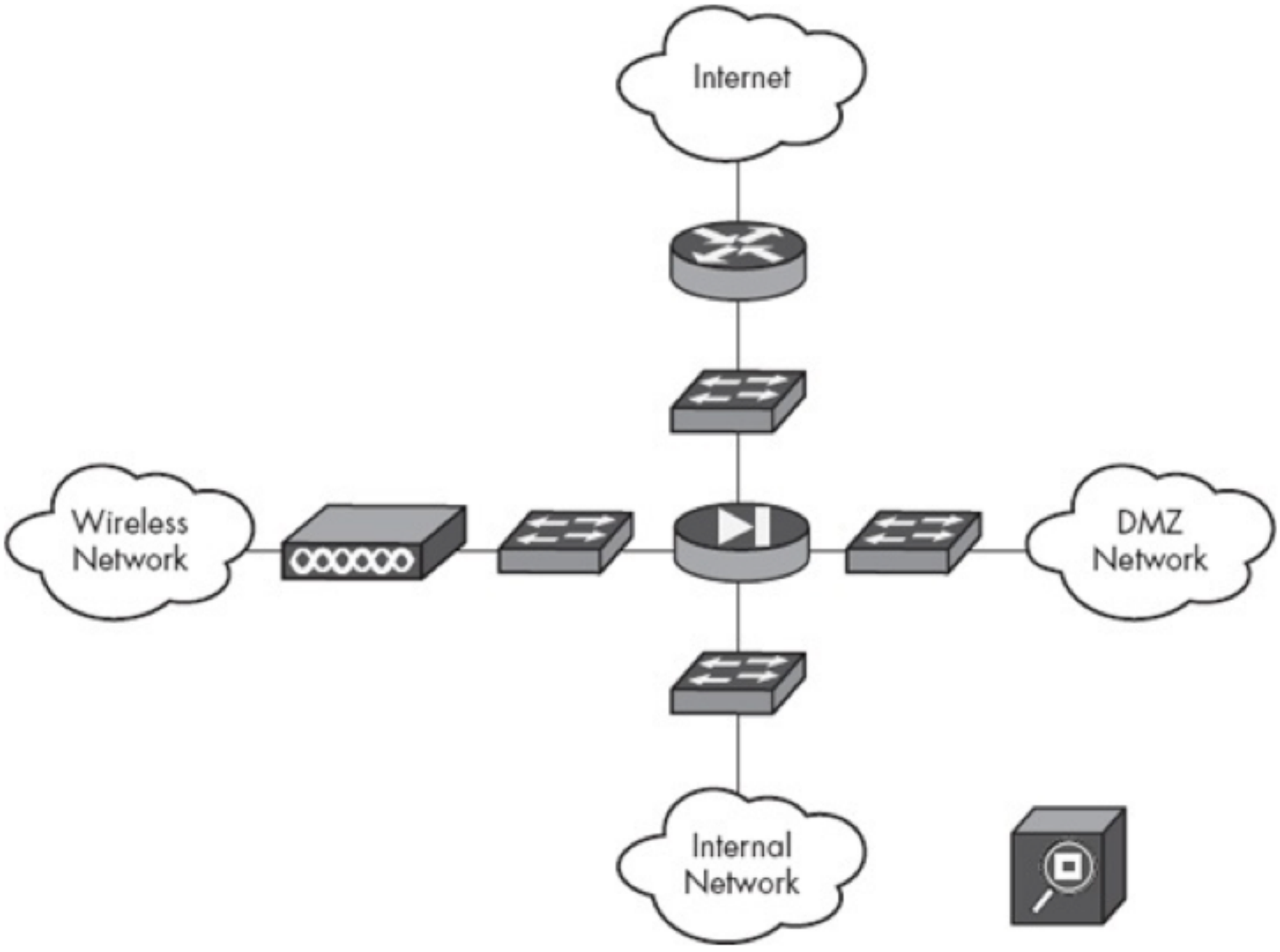


Figure 2-1. Vivian's Pets network

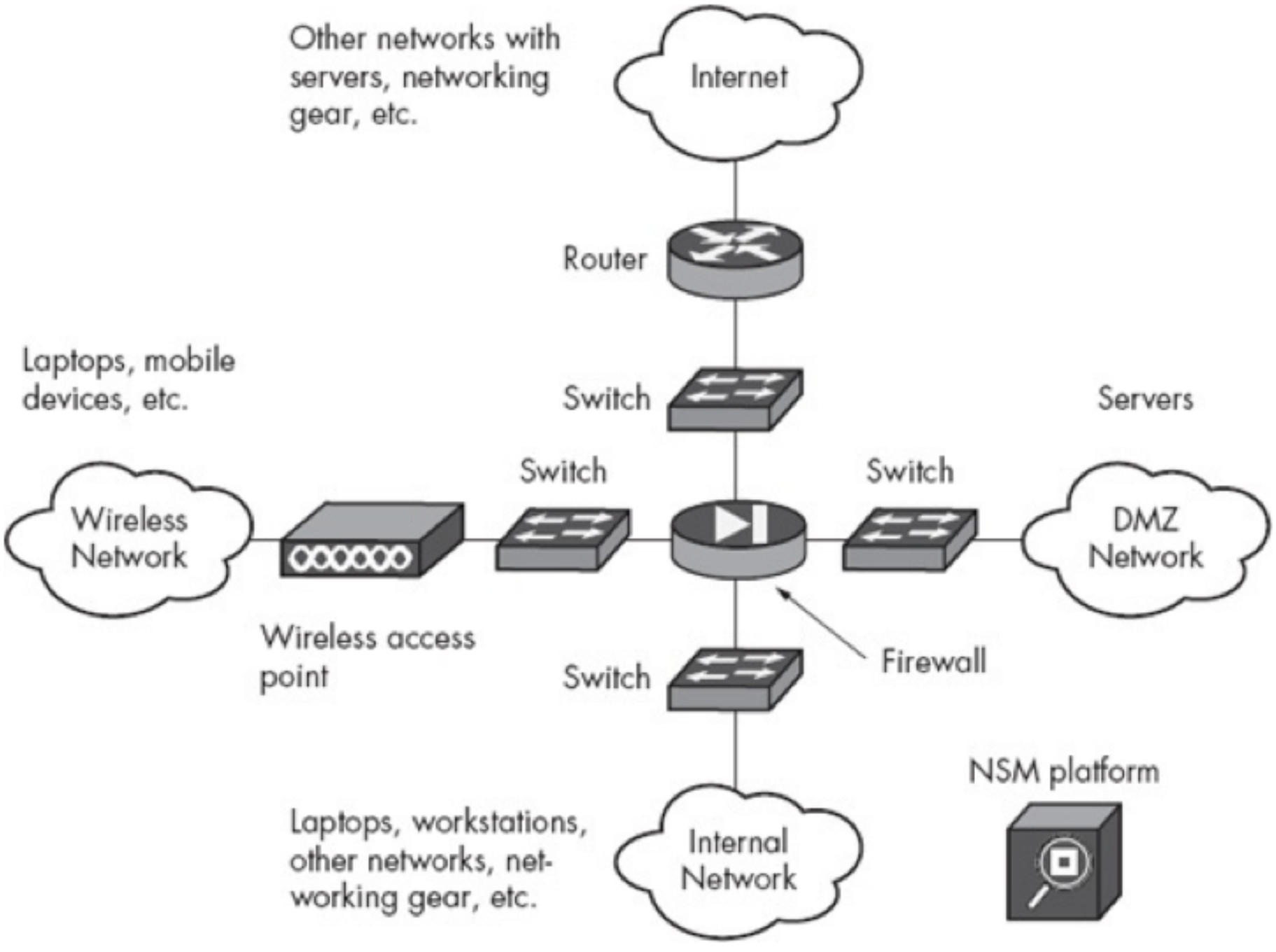


Figure 2-2. Vivian's Pets networking elements

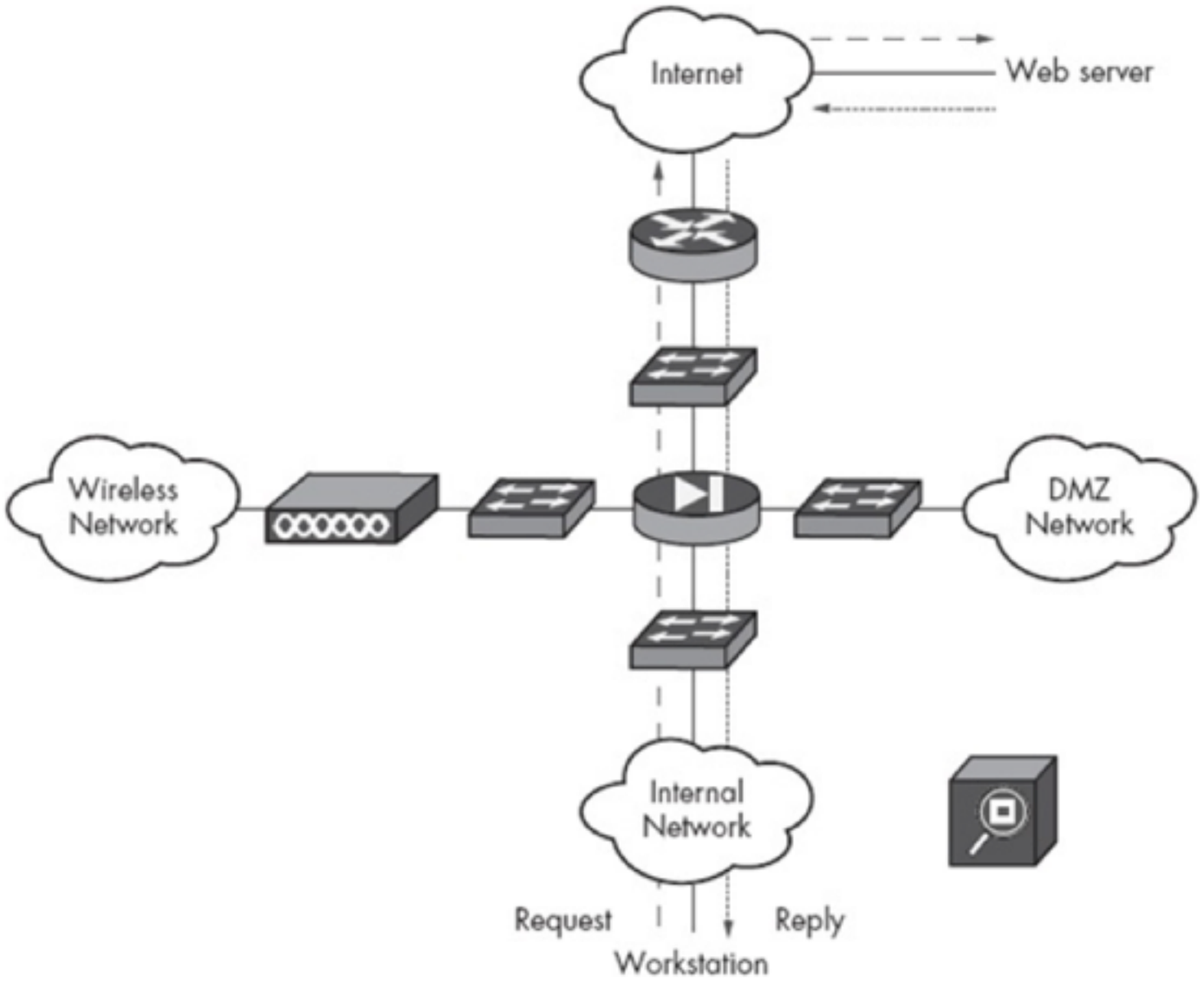


Figure 2-3. Network path from the workstation to the web server on the Internet

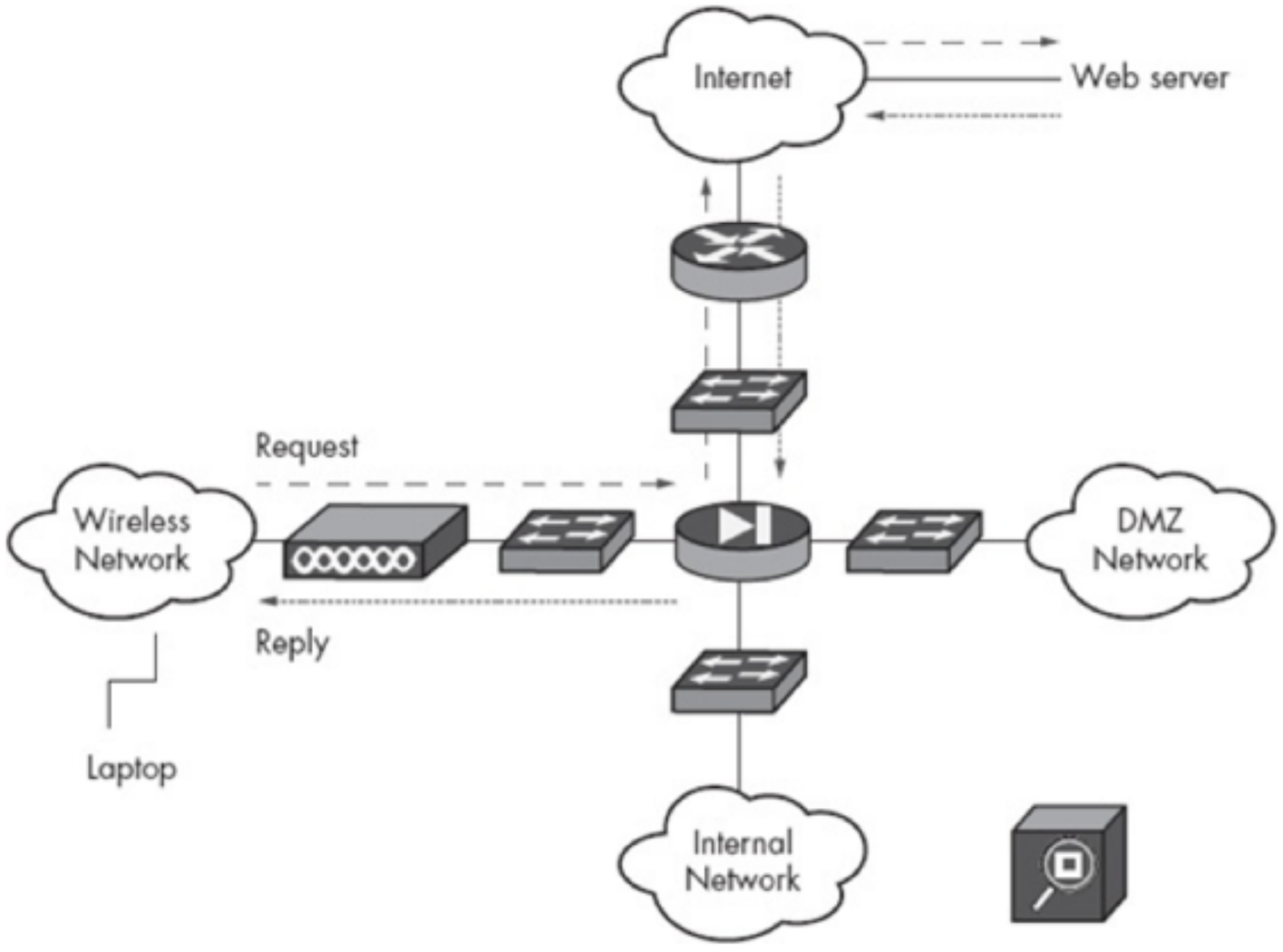


Figure 2-4. Network path from a laptop to a web server on the Internet

Issues

- **Company can only monitor traffic up to the external gateway**
  - **Beyond that point, only the ISP can monitor it**
- **Wireless traffic is usually encrypted at layer 2**
  - **More difficult to monitor than wired traffic**

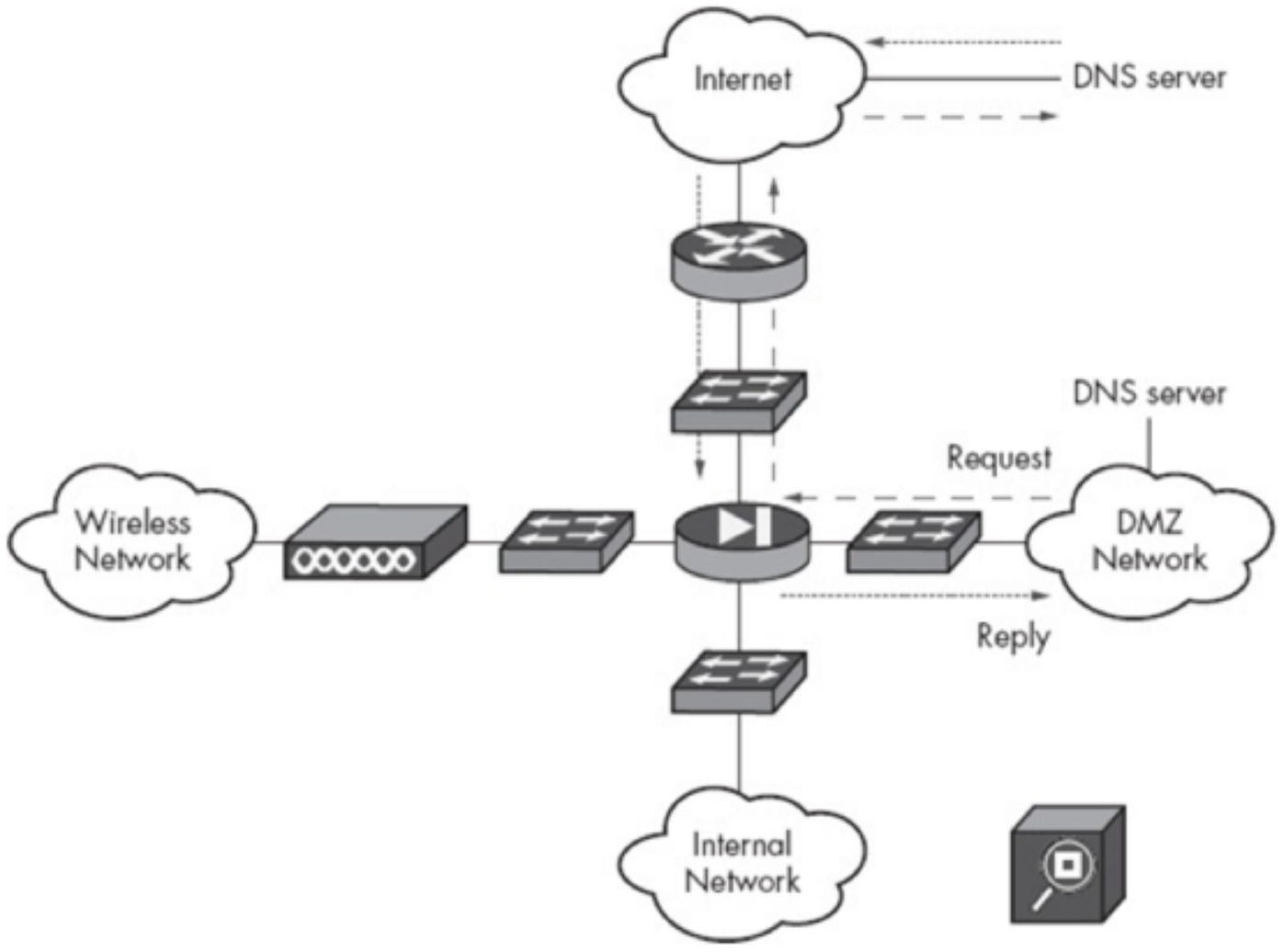


Figure 2-5. Network path from a local DNS server to a DNS server on the Internet

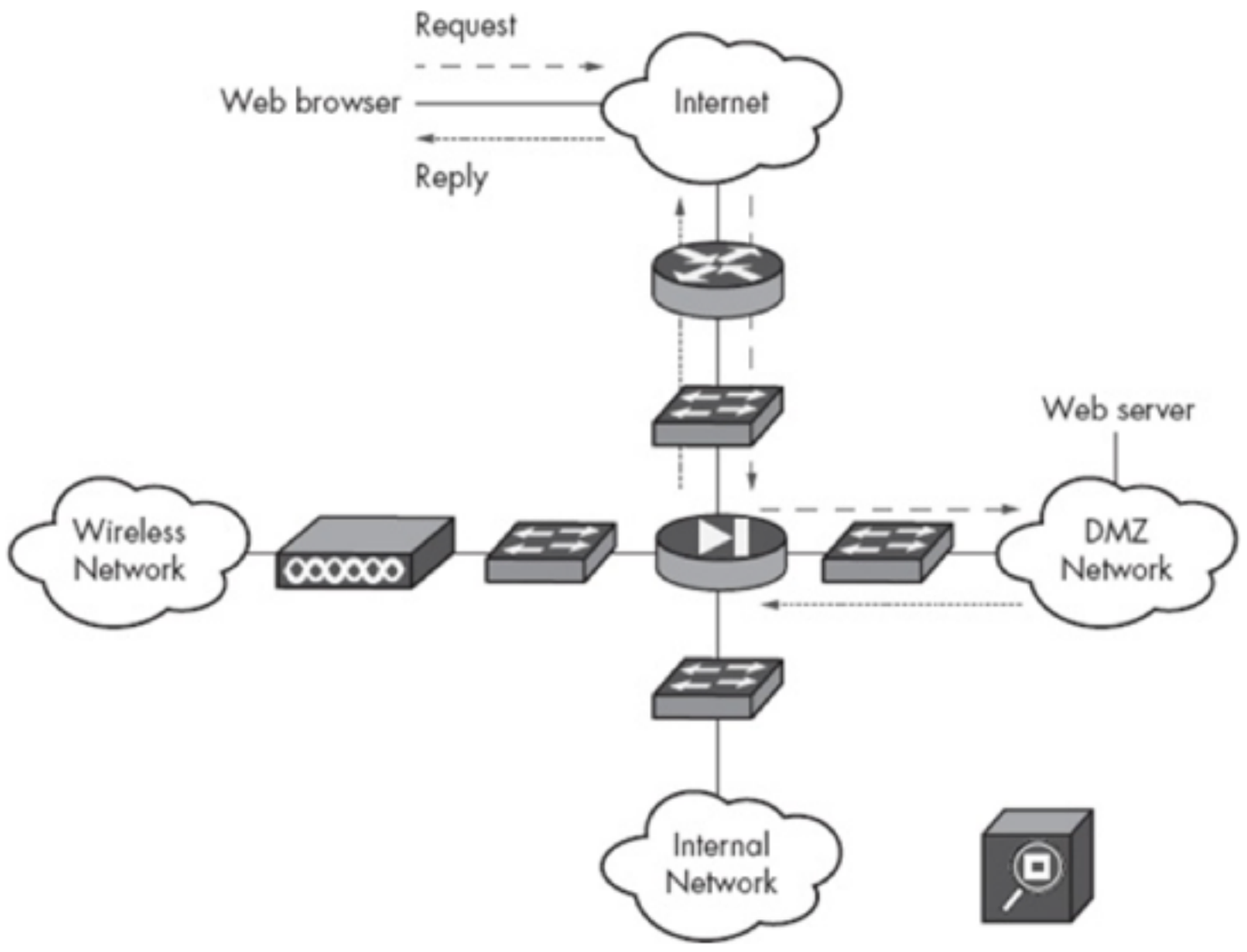


Figure 2-6. Network path from a web browser on the Internet to a web server hosted by Vivian's Pets

Issues

- **Devices on Wireless and Internal networks should be *clients*, not *servers***
  - **Should initiate connections, not receive them**
- **DMZ devices can act as either *clients* or *servers***
  - **May initiate or receive connections**

Other Traffic Flows

- Users on the internal network might access resources in the DMZ network.
- Users on the wireless network might access resources in the DMZ network.
- Systems in the DMZ network might access resources in the internal network.
- Systems in the wireless network might access resources in the internal network.

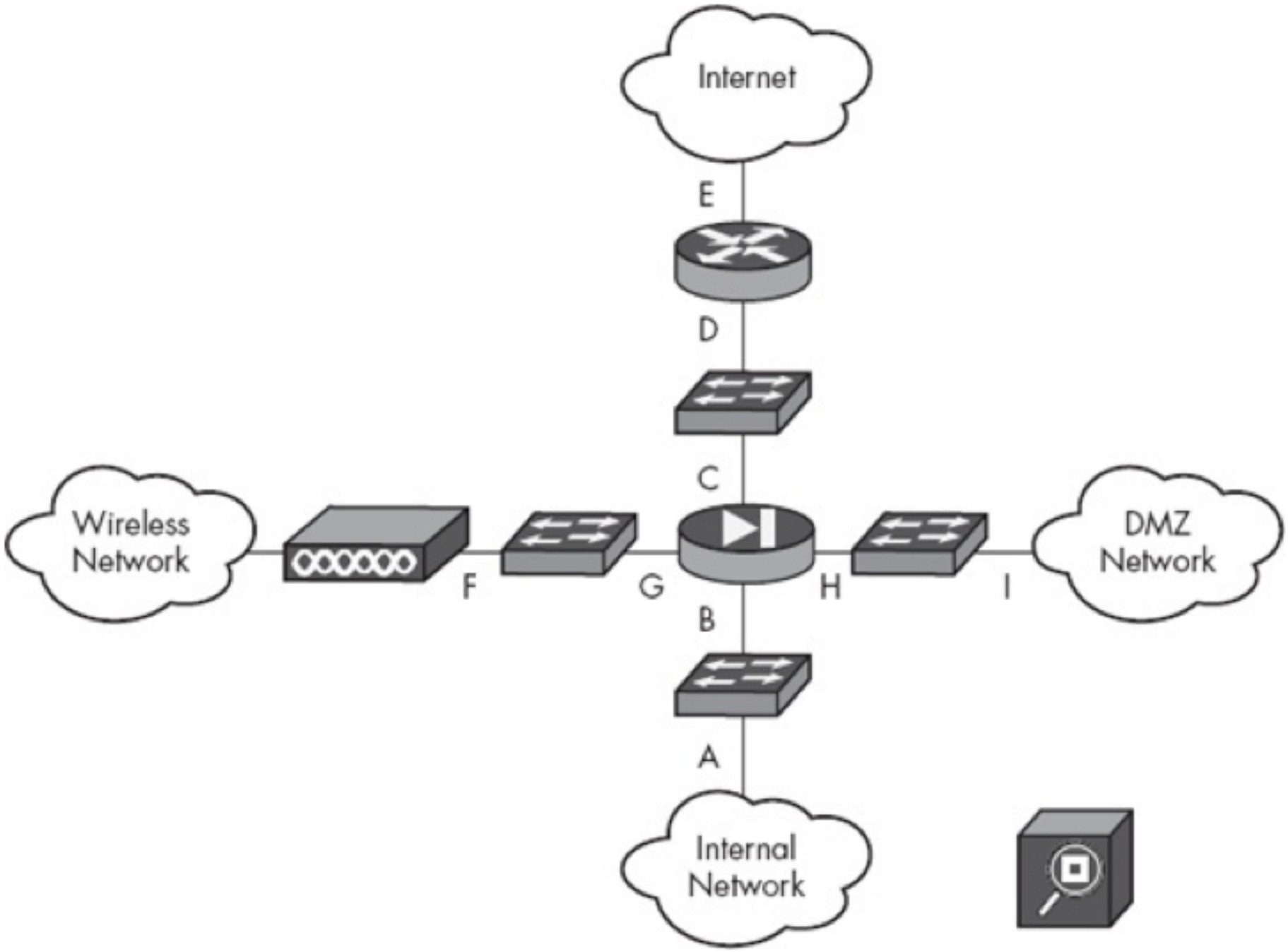


Figure 2-7. Monitoring location options

IP Addresses and Network Address Translation

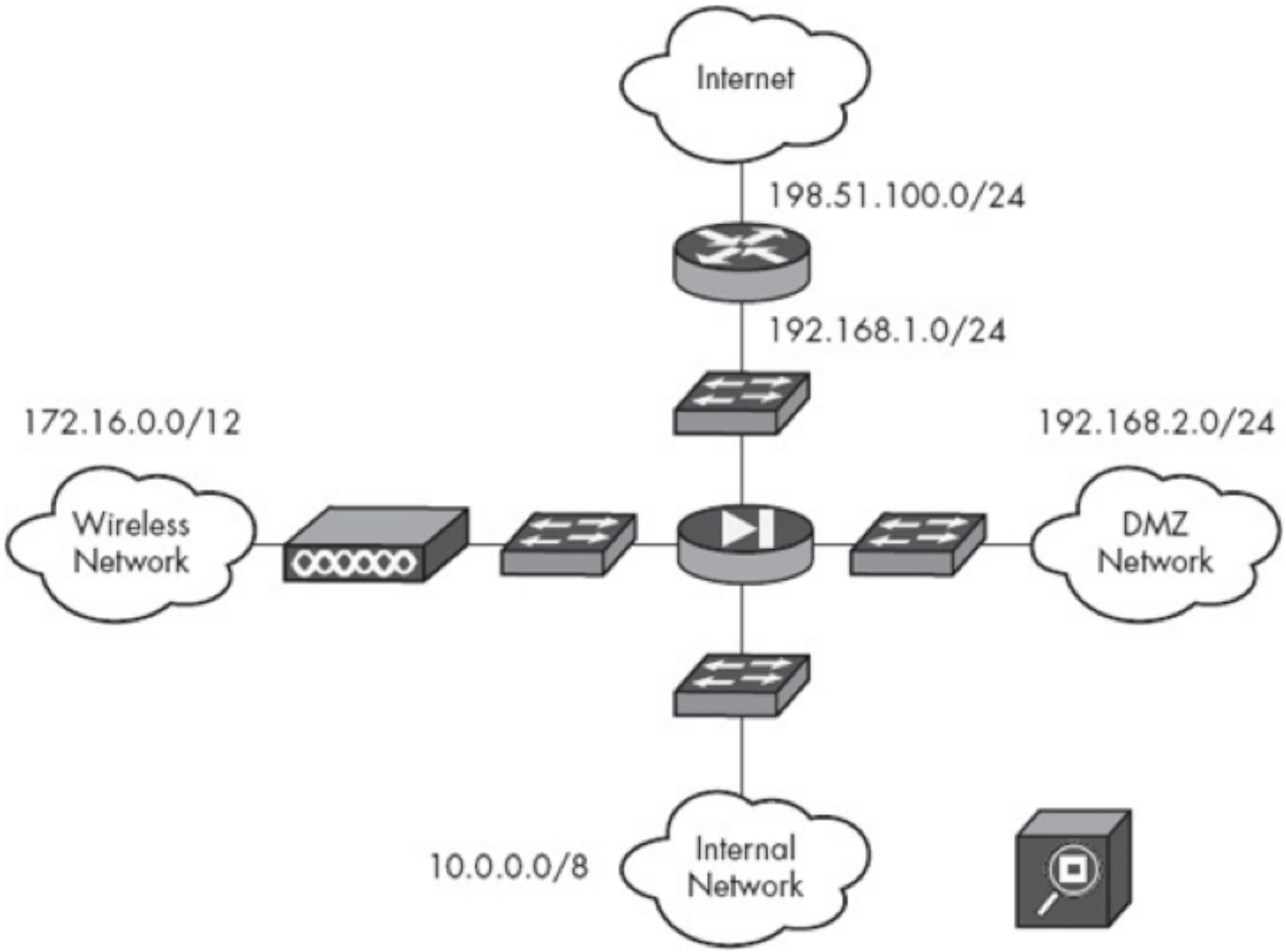


Figure 2-8. Net blocks assigned to segments

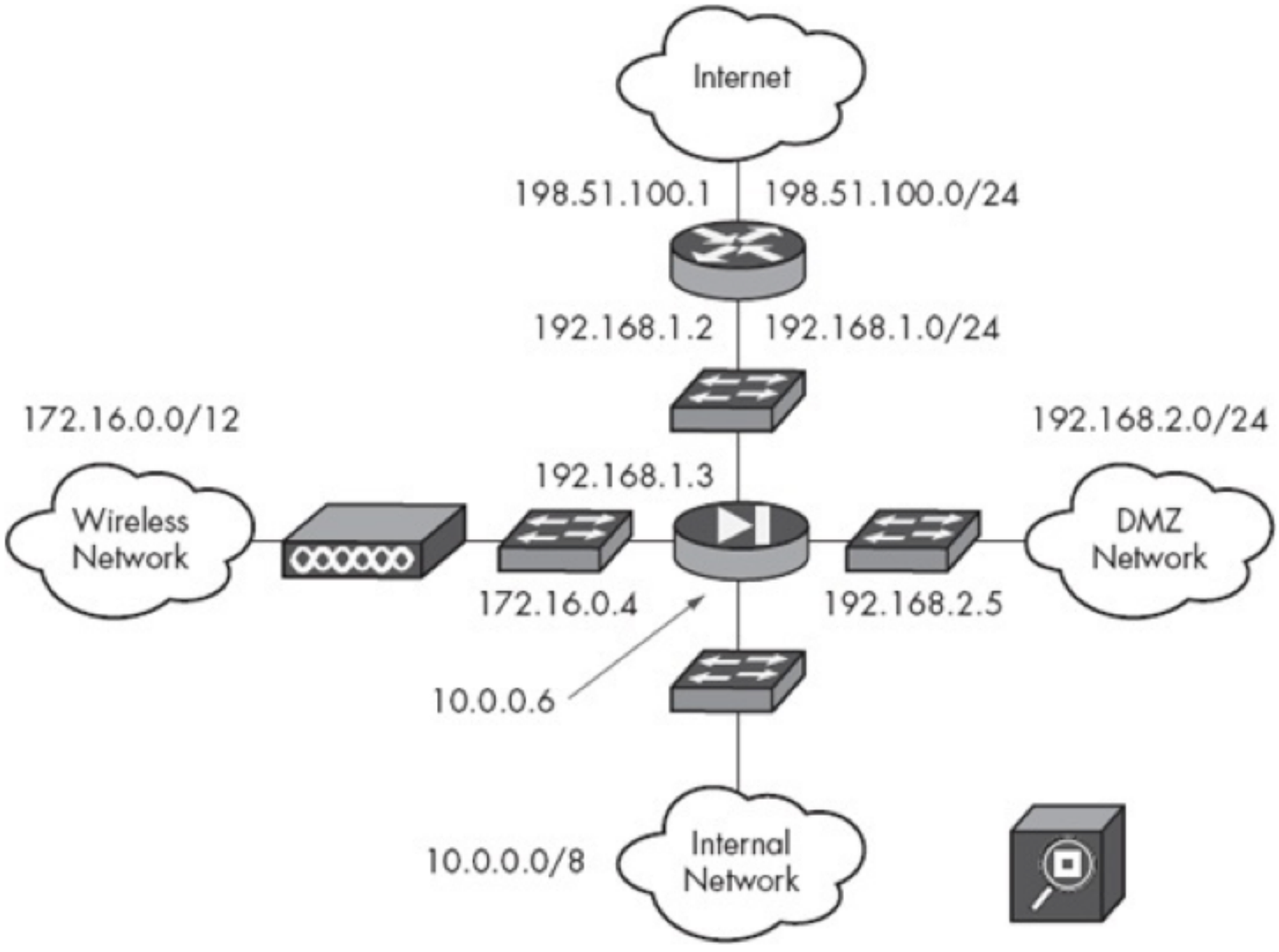


Figure 2-9. IP addresses assigned to key devices

Network Address Translation (NAT)

- **Private IP addresses cannot be used on the Internet**
  - **192.168.0.0 - 192.168.255.255**
  - **172.16.0.0 - 172.31.255.255**
  - **10.0.0.0 - 10.255.255.255**
- **They must be *translated* to public IP addresses**
- **Often done at the firewall or gateway to the Internet**

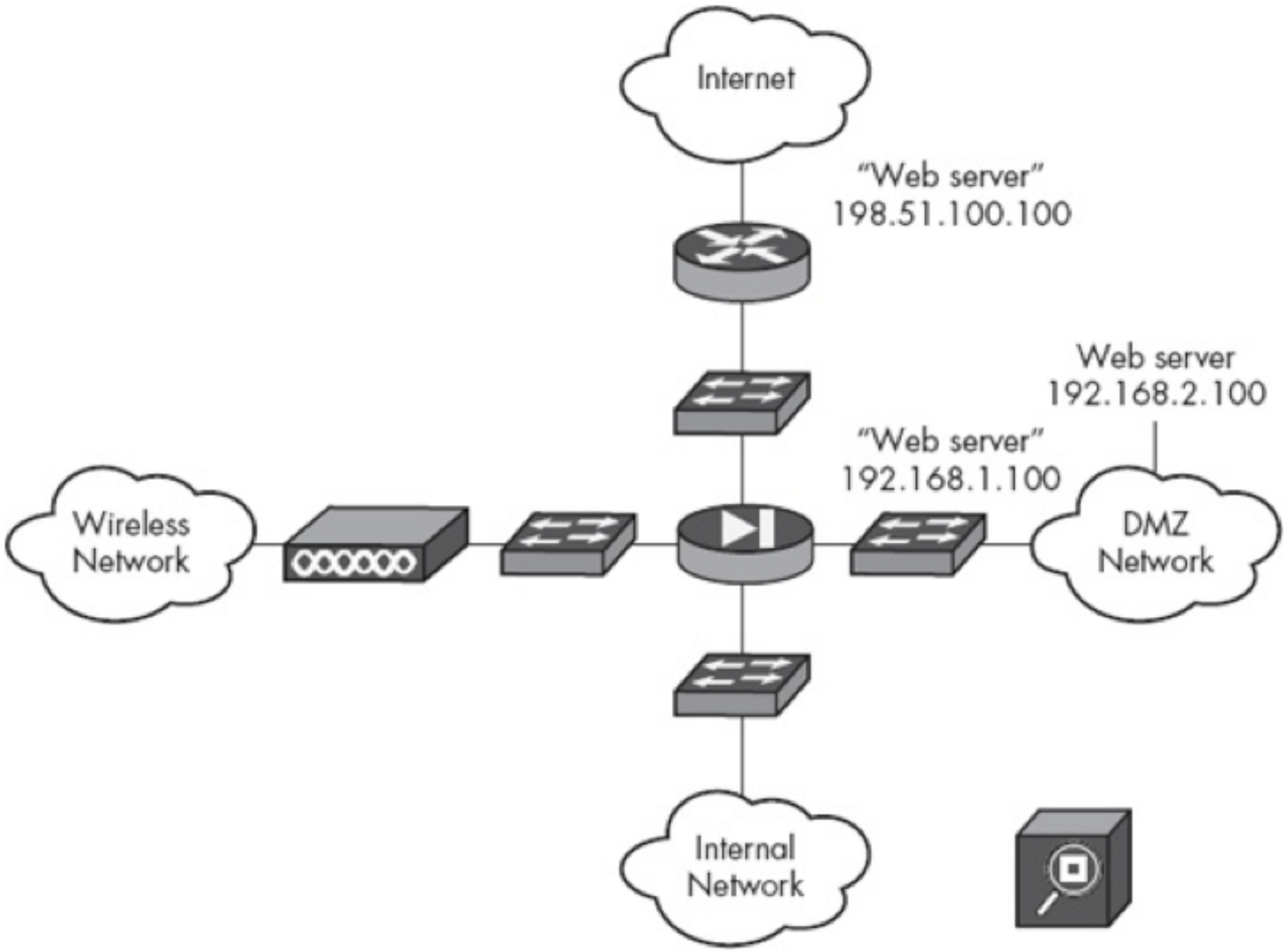


Figure 2-10. NAT of the web server in the DMZ network

One-to-One Mapping

- **The diagram in the previous slide shows this technique**
- **A public IP is offering a service on port 100**
- **It's actually forwarded to a machine in the DMZ with a local address**
- **This requires a different public IP for each server (expensive)**

Network Port Address Translation (NPAT or PAT)

- **Multiple local addresses share a single public IP address**
- **Each connection gets a different public port number**
- **Works for clients, but not for servers**
- **Appropriate for Wireless and Internal networks**
- **Consumes fewer public IPs, but increases load on firewall and gateway**

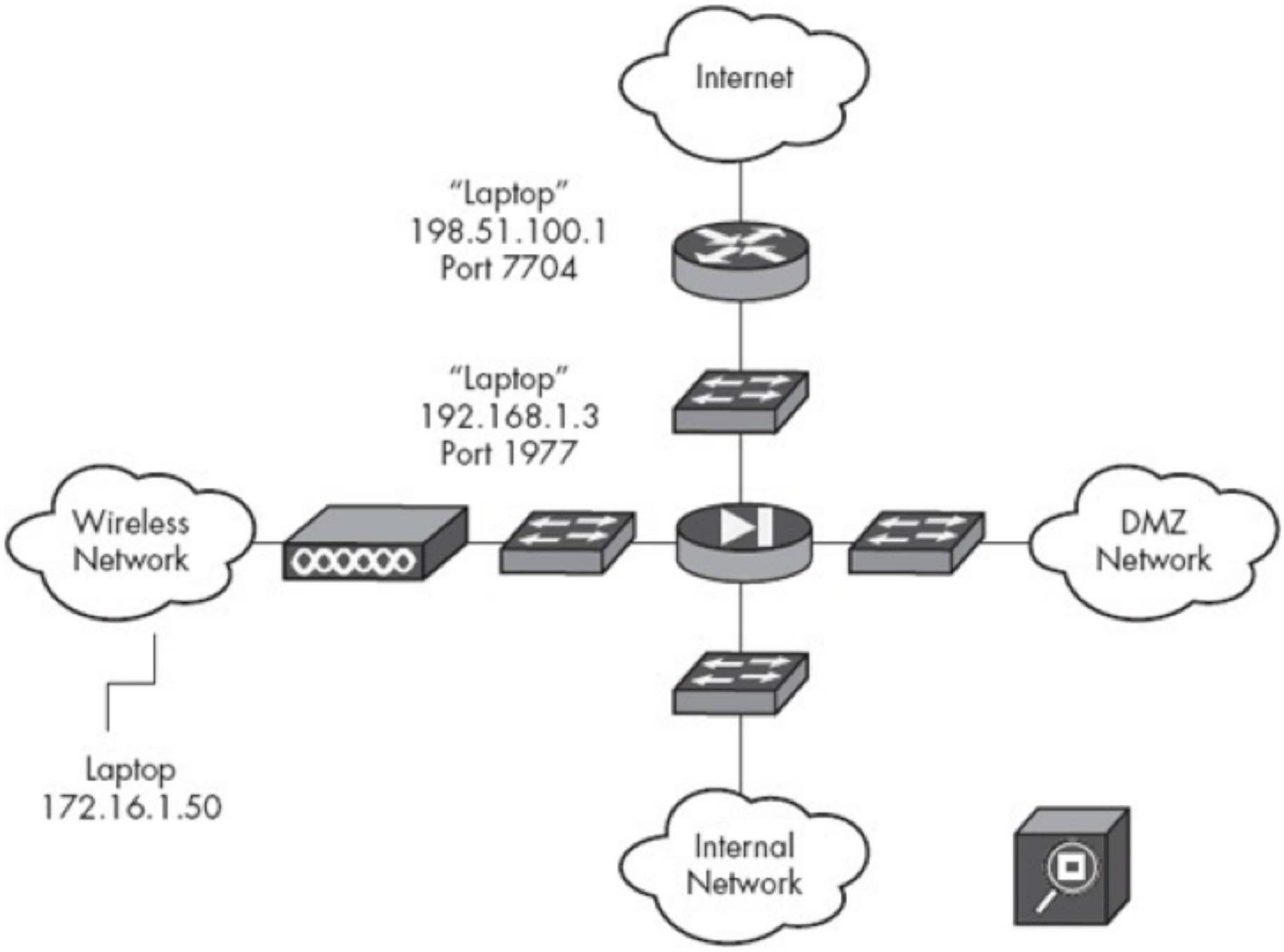


Figure 2-11. NPAT of a laptop in a wireless network


Kahoot!

Choosing the Best Place to Obtain Network Visibility

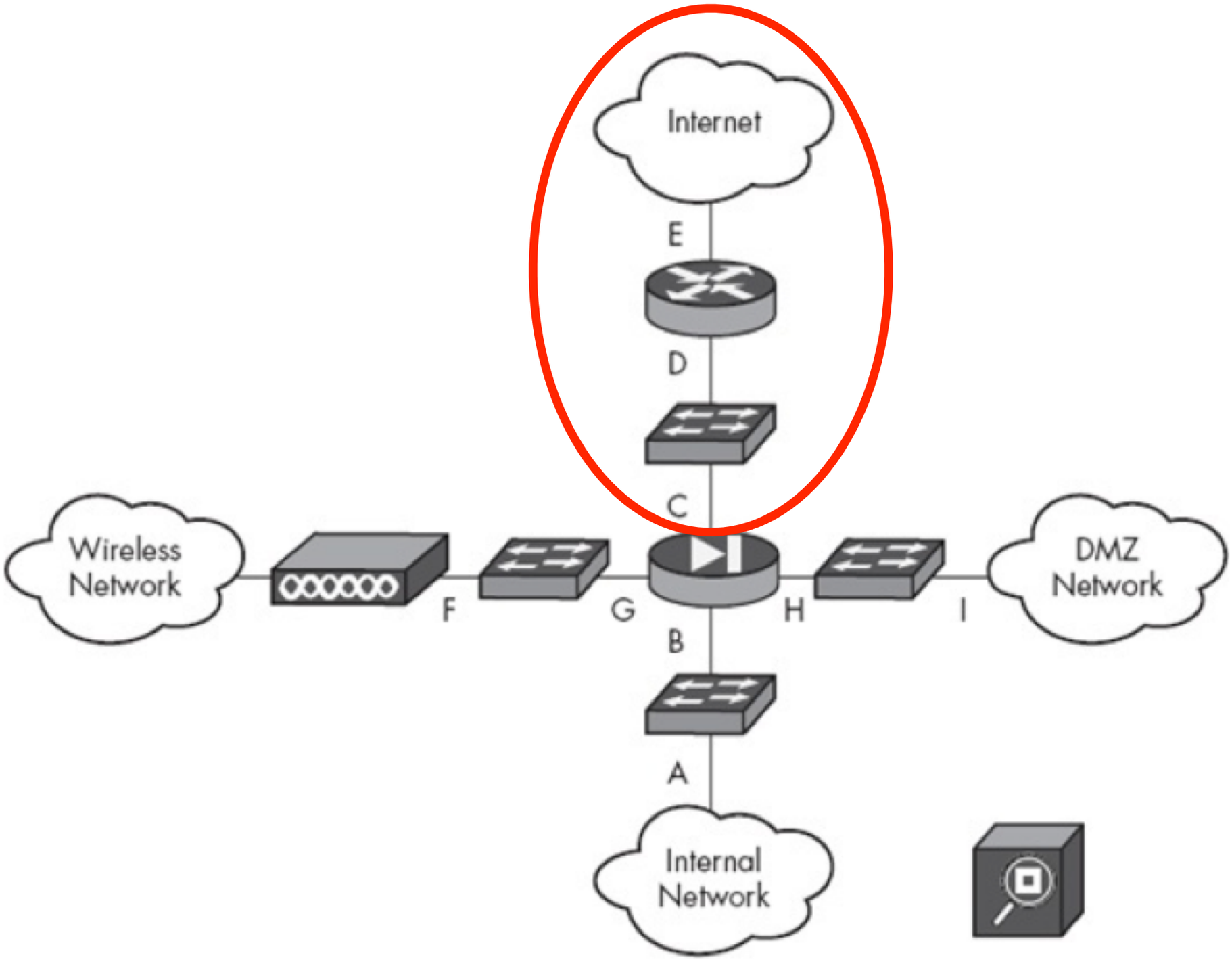


Figure 2-7. Monitoring location options

WAN Locations

- **Locations C, D, and E**
- **All on the public side of the firewall**
- **After NAT: local IP addresses have been removed**
- **Difficult to identify the local device sending or receiving data**
- **Easier for DMZ zone because of one-to-one mapping**

Wireless Traffic

Location C

This is at the firewall's interface facing the Internet. All NPAT'd traffic has a source IP address of 192.168.1.3.

Location D

This is between the firewall's interface facing the Internet and the gateway's interface facing the company. All NPAT'd traffic also has a source IP address of 192.168.1.3.

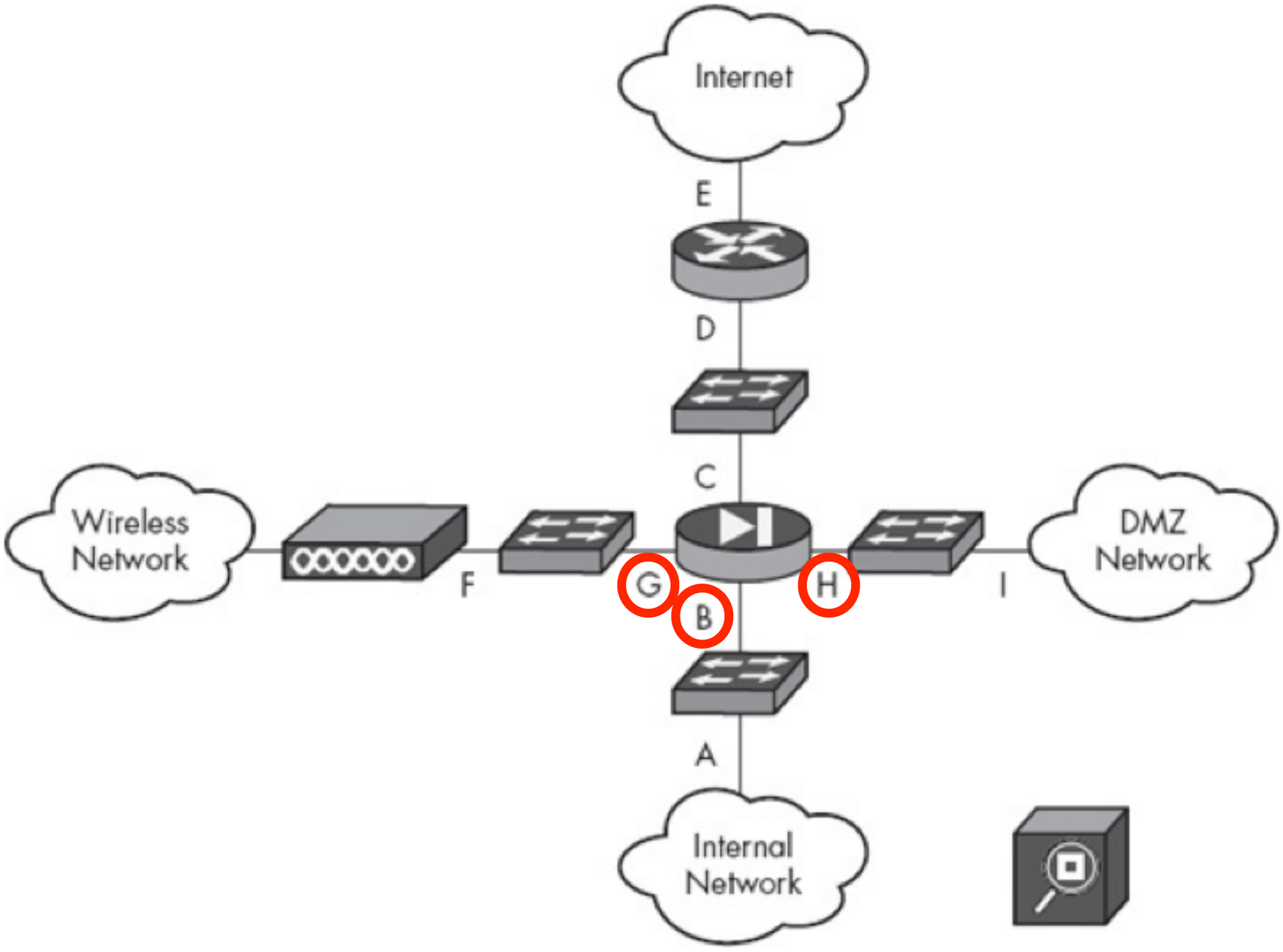
Location E

This is between the gateway's interface facing the Internet and the Internet. All NPAT'd traffic has a source IP address of 198.51.100.1.

Sensor Placement Options

- **There is no single place that lets us see true source IP addresses for all networks**
  - **Unless the firewall is configured to send copies of all traffic to an NSM platform**
  - **But this links the different segments together, which is risky**
- **Better option: deploy three sensors**

Deploy Three Sensors



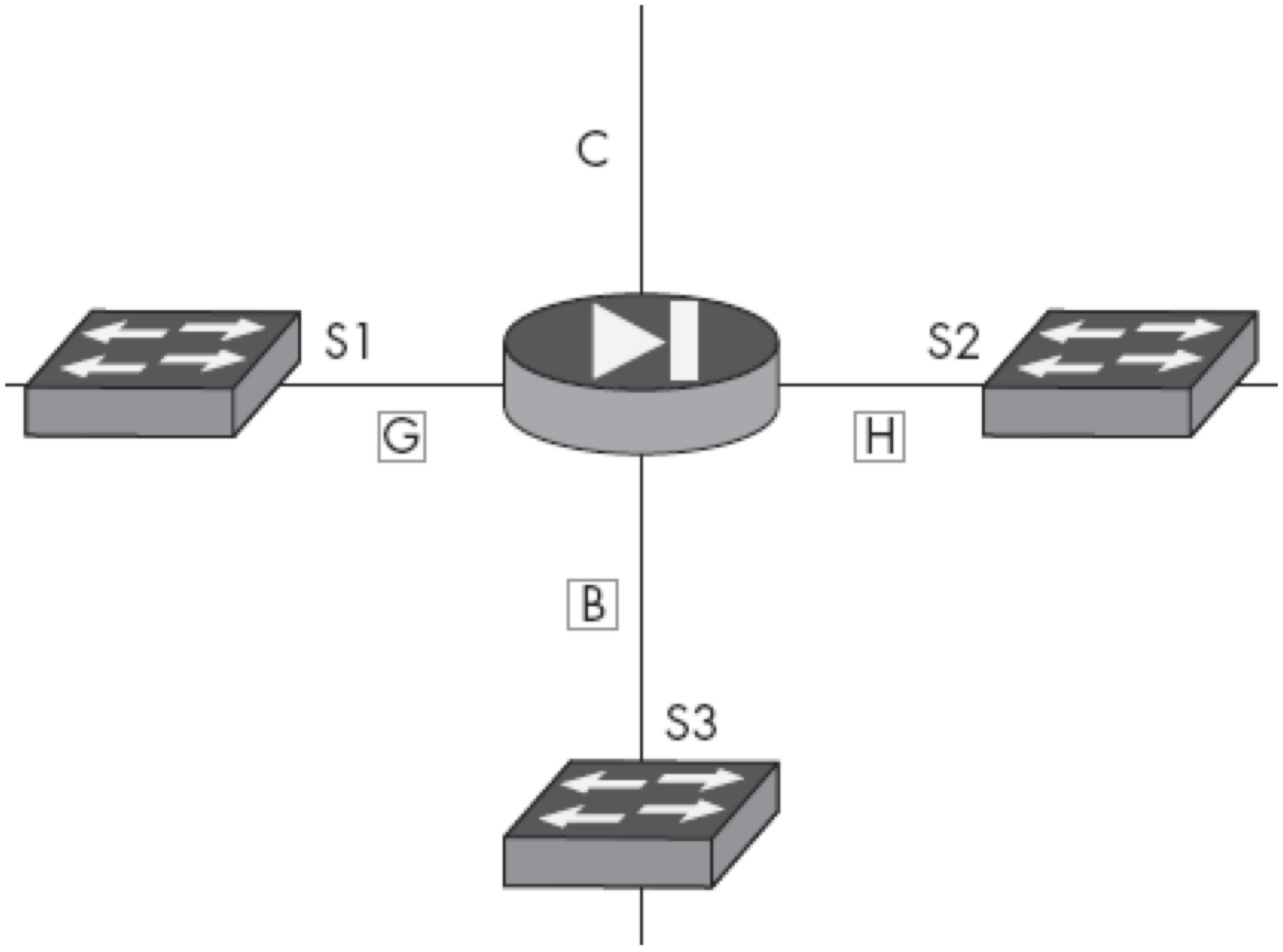
Getting Physical Access to the Traffic

Using Switches for Traffic Monitoring

- **Configure switches to send a copy of trafffic to a port for monitoring**

- **Cisco calls this SPAN (Switched Port Analyzer)**

- **Juniper & Dell call it *port mirroring***


C
S1
S2
G
H
B
S3

Using a Network Tap

- **Recommended option**
- **Easier to install and maintain than SPAN ports**
- **Which can be disabled, misconfigured or oversubscribed**

Capturing Traffic on a Firewall or Router

- **Might be useful for short-term troubleshooting**
- **Not a viable long-term solution**
- **Because filtering and routing platforms lack robust storage media**

Capturing Traffic Directly on a Server

- **May be the only option for CIRTs (Computer Incident Response Teams)**

- **Especially when servers are in the cloud**

Capturing Traffic Directly on a Client

- **Might work for temporary storage**
- **But not appropriate for long-term collection of network data**
- **Too limited and data is spread across many devices**

Choosing an NSM Platform

NSM Platform

- **The server connected to the network tap**
- **Runs NSM tools to collect and analyze traffic**
- **Can be a commercial appliance, a self-built system, or a virtual machine**

NSM Platorm Characteristics

- **Large RAIDs to store data**
- **RAM: 4 GB + 1GB per monitored interface**
- **One CPU per monitored interface**
- **Multiple network interfaces to connect to SPAN ports or taps**

Estimating Data Storage Requirements

- **Multiply these together to get daily storage needed**
  - **Average network utilization in Mbps**
    - **1 byte / 8 bits**
    - **60 seconds per minute**
    - **60 minutes per hour**
    - **24 hours per day**

Estimating Data Storage Requirements

- **Example:**
  - **100 Mbps * 1/8 * 60 * 60 * 24 = 1.08 TB per day**
  - **45 GB per hour**
  - **32 TB per 30 days**
- **Add 10% more for databases**
- **And 5% more for text files**
- **38 TB for a month of data**

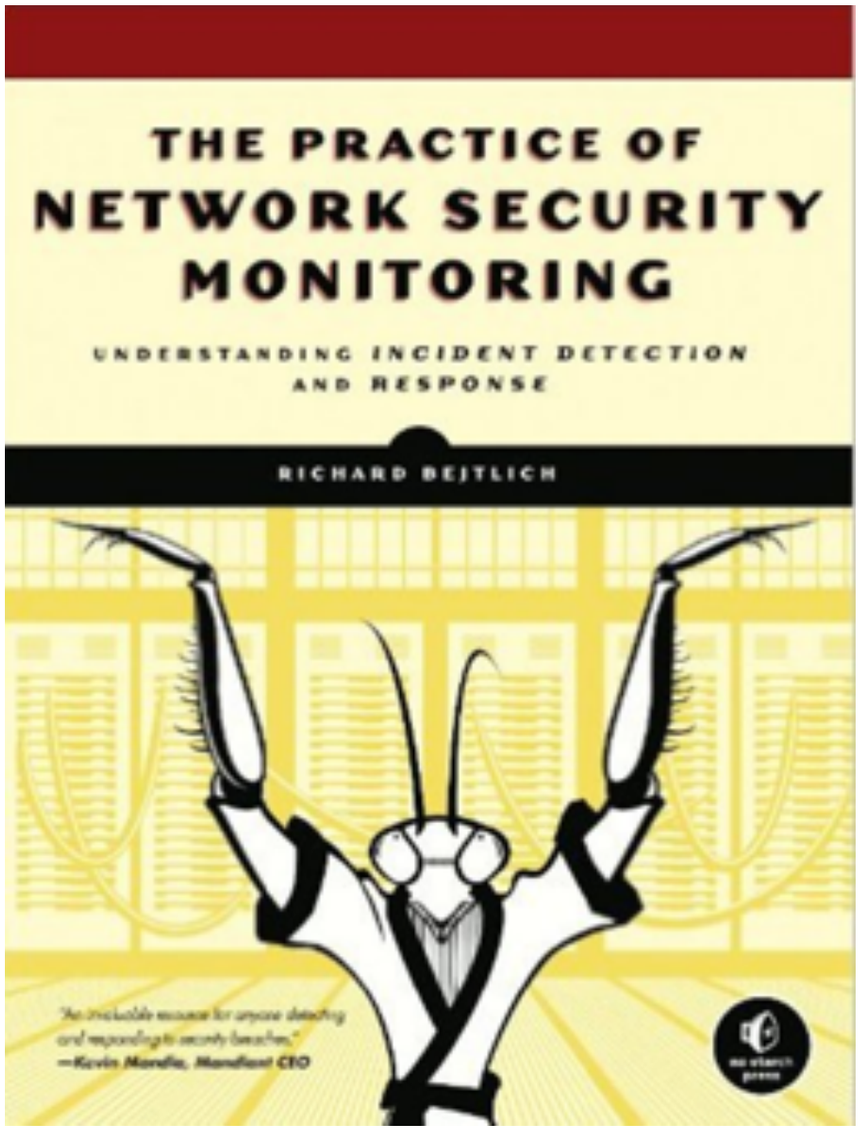
Ten NSM Platform Management Recommendations

1. Limit command shell access to the system to only those administrators who truly need it. Analysts should log in to the sensor directly only in an emergency. Instead, they should access it through tools that allow them to issue commands or retrieve data from the sensor.
2. Administrators should never share the root account, and should never log in to sensors as the root account. If possible, access the sensor using shared keys, or use a two-factor or two-step authentication system like Google Authenticator.
3. Always administer the sensor over a secure communications channel like OpenSSH.
4. Do not centrally administer the sensor's accounts using the same system that manages normal IT or user assets.
5. Always equip production sensors with remote-access cards.

6. Assume the sensor is responsible for defending itself. Limit the exposure of services on the sensor, and keep all services up-to-date.
7. Export logs from the sensor to another platform so that its status can be remotely monitored and assessed.
8. If possible, put the sensor's management interface on a private network reserved for management only.
9. If possible, use full disk encryption to protect data on the sensor when it is shut down.
10. Create and implement a plan to keep the sensor software up-to-date. Treat the system like an appliance, but maintain it as a defensible platform.

CNIT 50:
Network Security Monitoring

3. Standalone NSM Deployment and Installation



Topics

- **Stand-alone or Server Plus Sensors?**
- **Choosing How to Get SO Code onto Hardware**
- **Installing a Stand-alone System**

Stand-alone or Server Plus Sensors?

Two Deployment Modes

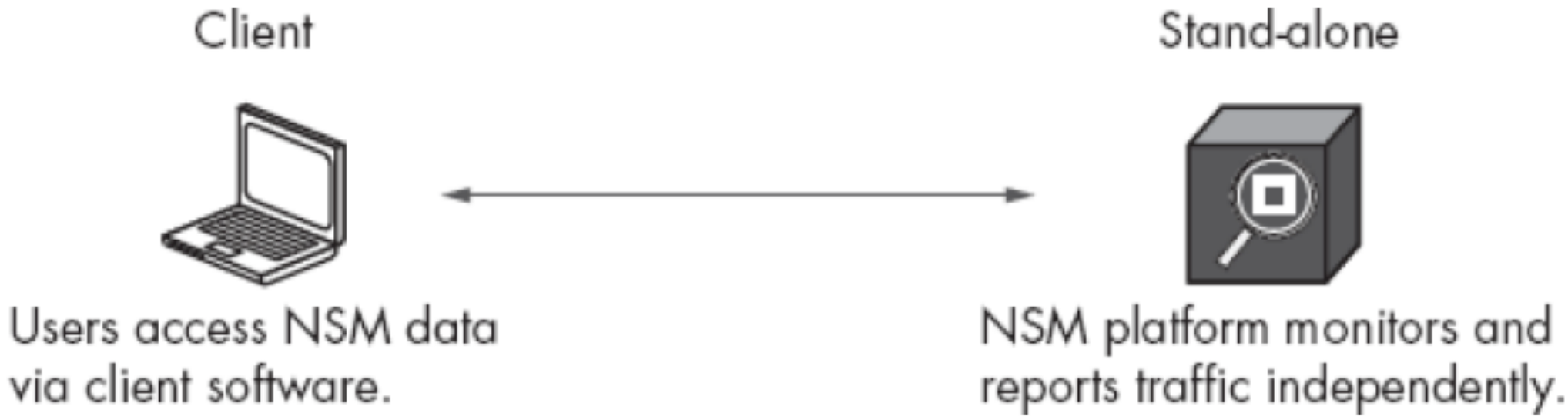
Stand-alone mode

In this mode, SO is a self-contained, single-box solution that collects and presents data to analysts.

Server-plus-sensors mode

In this mode, SO acts as a distributed platform, with sensors collecting data and a server aggregating and presenting data to analysts.

Stand-alone



- **Best for beginners**
- **All traffic goes to one NSM platform**
- **Good for networks with simple NSM requirements**

Stand-alone

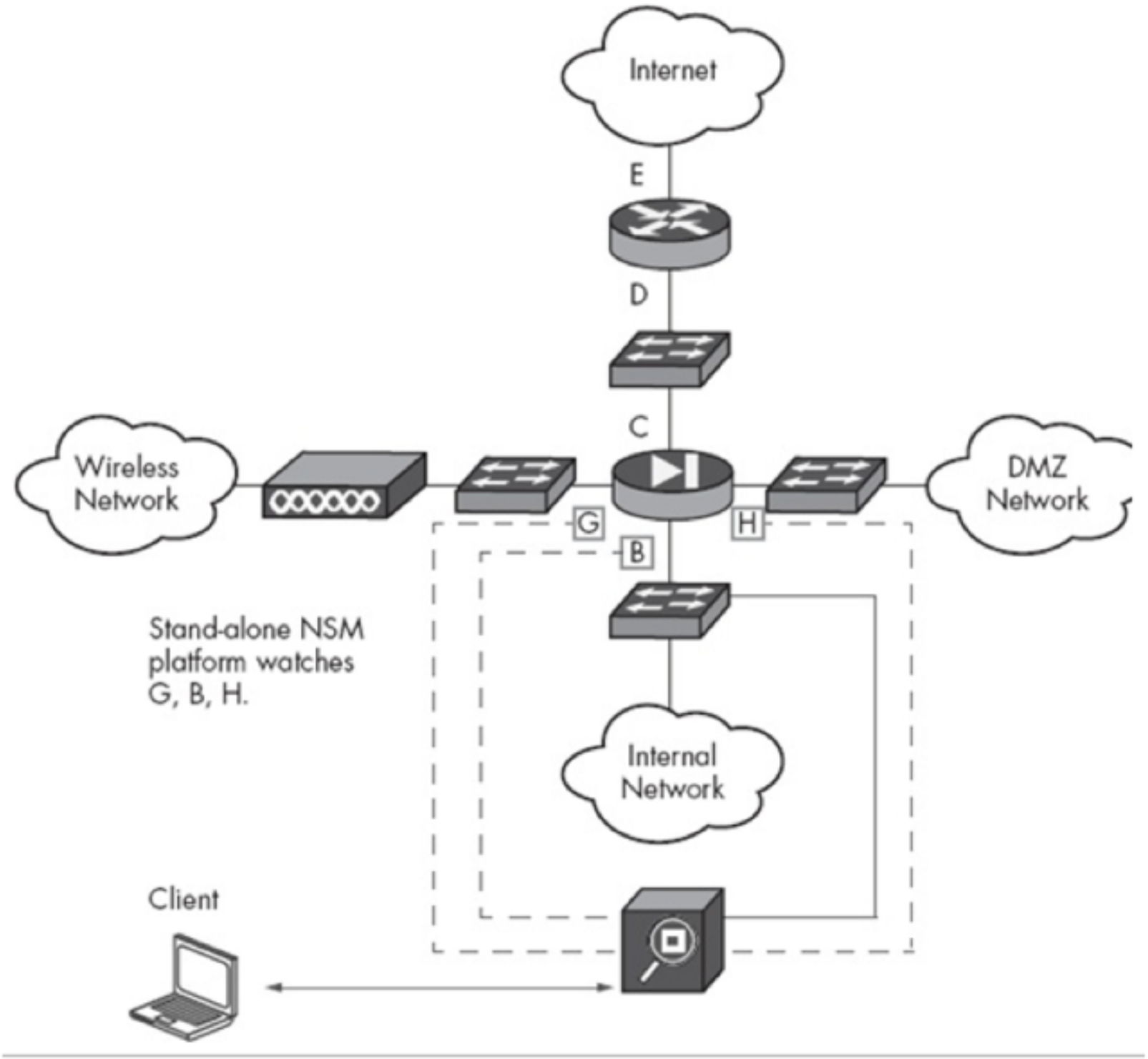
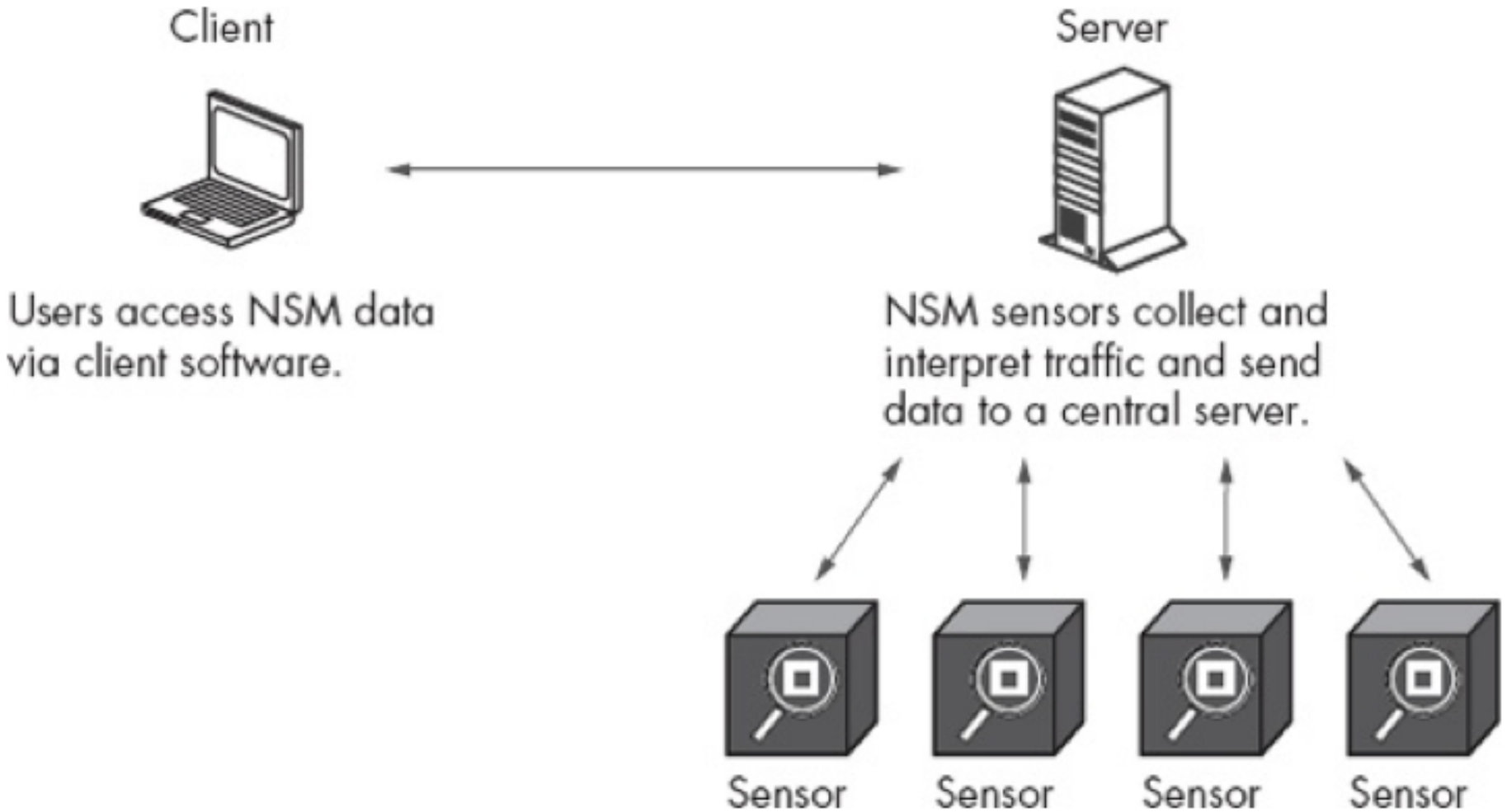


Figure 3-2. Stand-alone SO platform watches network locations G, B, and H.

Server-Plus-Sensors



- **Distributes NSM duties across several servers**
- **For larger, more complex networks**
- **Such as geographically separate networks**

Server-Plus-Sensors

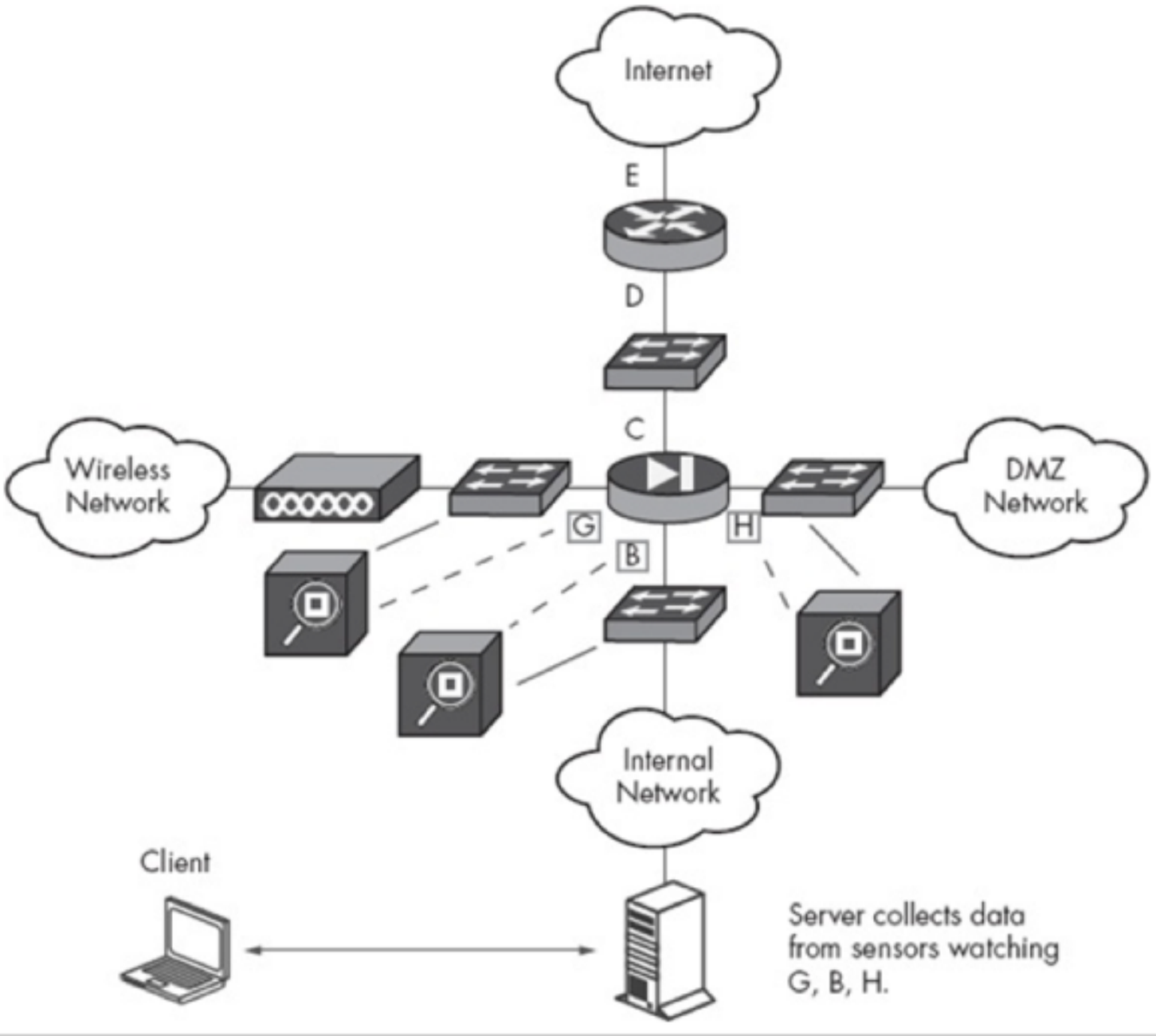


Figure 3-4. The SO server collects data from sensors watching network locations G, B, and H.

Global Deployment

- **In server-plus-sensors mode**
  - **Sensors don't need to be within the local network**
  - **Can be deployed globally**
  - **Connect back to central server via the network**
  - **Through a VPN or through public mangement interfaces**

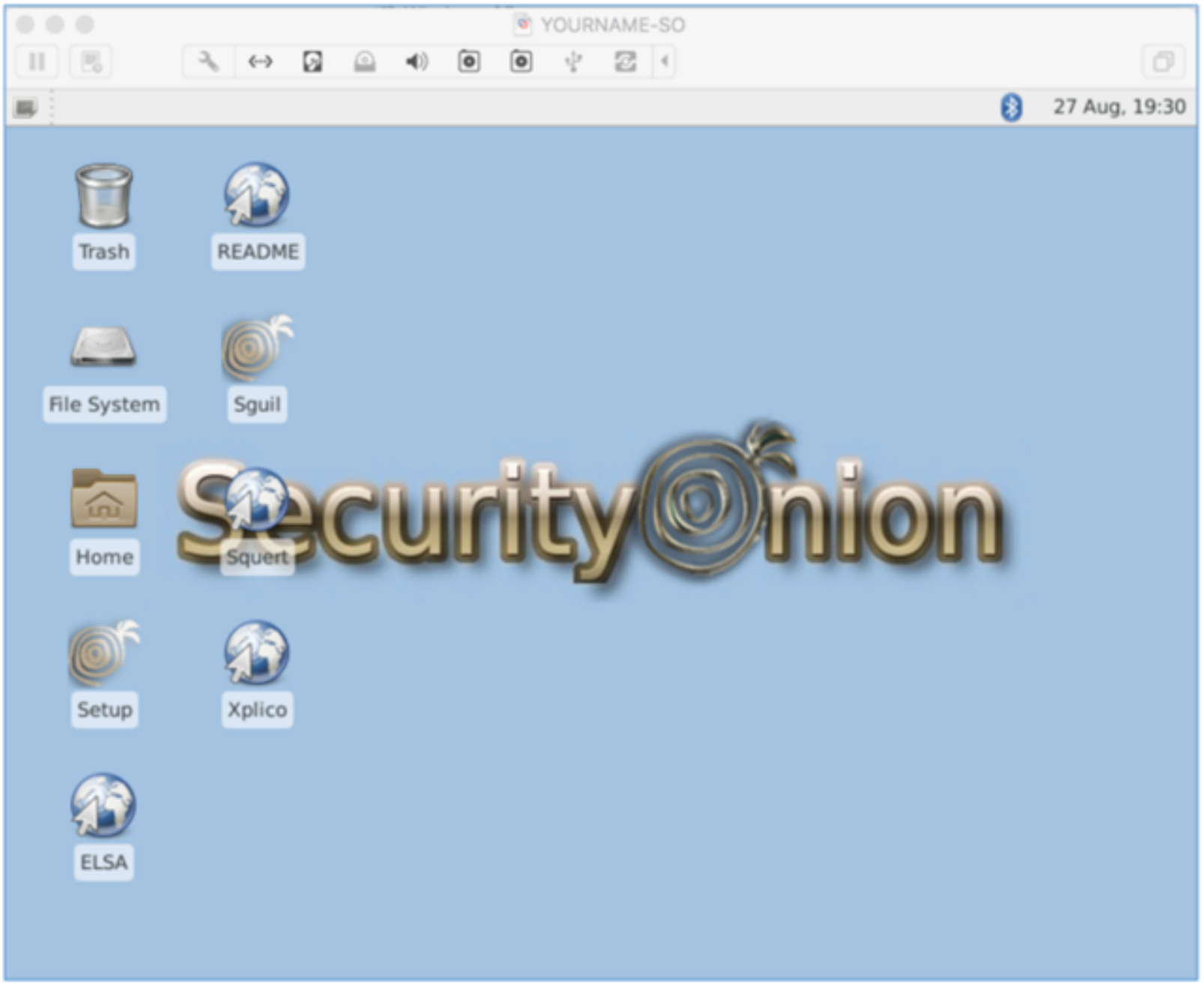
Choosing How to Get SO Code onto Hardware

Hardware

- **SO supports two ways to install code**
  - **Download ISO file and install from it**
    - **Flash it to a DVD or thumbdrive**
- **Ubuntu Personal Package Archives (PPA)**
  - **Can install SO on Ubuntu, or derivatives like Xubuntu (64-bit)**

Installing a Stand-alone System

Project 1


YOURNAME-SO
27 Aug, 19:30
Trash
README
File System
Sguil
Home
Squert
SecurityOnion
Setup
Xplico
ELSA


Kahoot!