ENPM 686 FINAL PROJECT

Vivian Choe
ENPM 686 - Information Assurance
Spring 2016

OVERVIEW

- Budget breakdown: $500K
- Network Design: Before & After
- Incident Response Framework
- Threat Management System
- Intrusion Detection System
- Intrusion Prevention System
- Hardening of OS & Web Server

$$ BUDGET BREAKDOWN $$

- Security administrator: $75K
- Network Improvements: $100K
- IDS System: $150K (Network & Host)
- IPS System: $150K (Network & Host)

Only estimated budget figures

NETWORK DESIGN: BEFORE

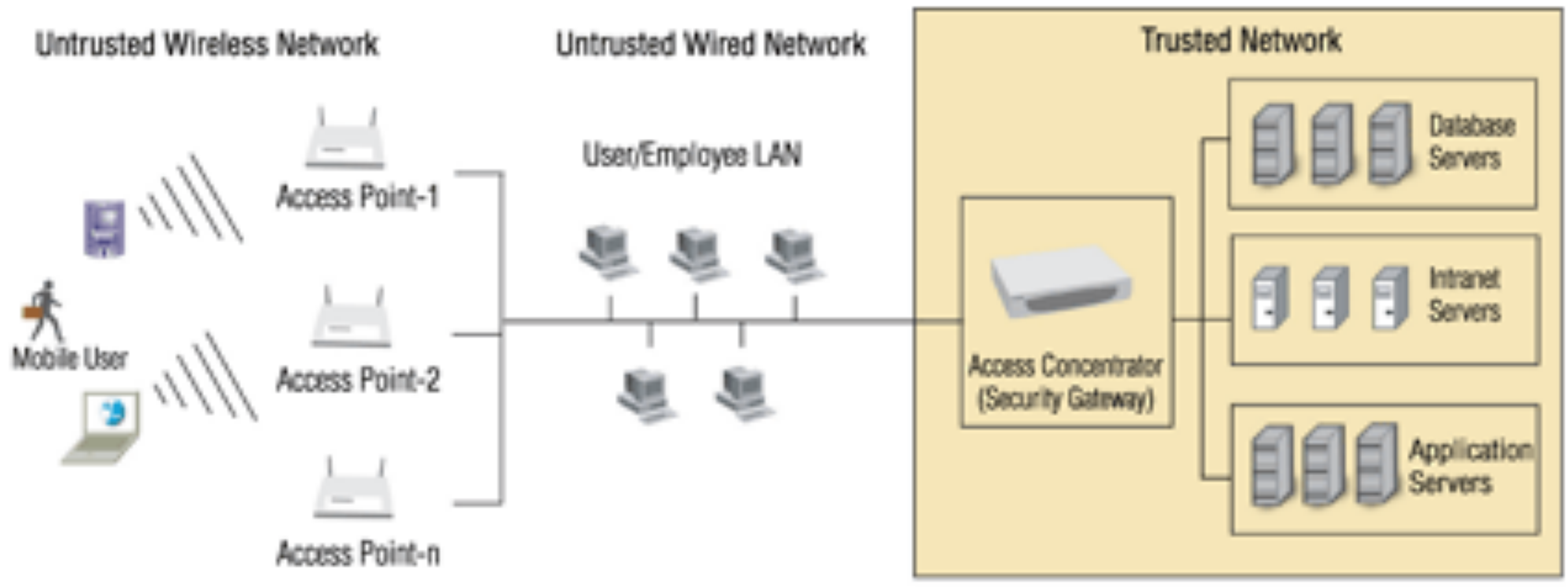


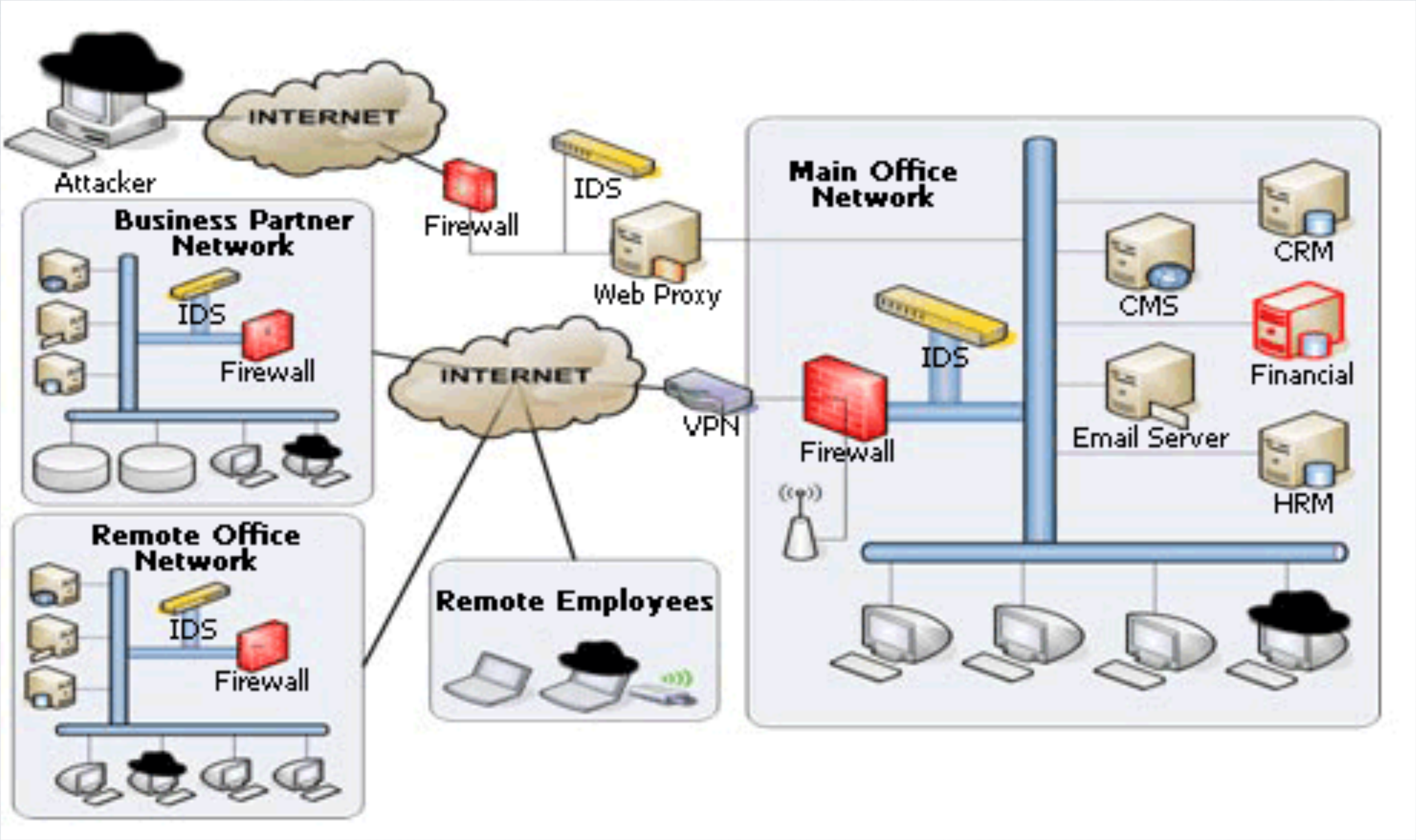
Figure 1 A typical enterprise network deployment scenario.

Network susceptible to attacks

NETWORK DESIGN: BEFORE

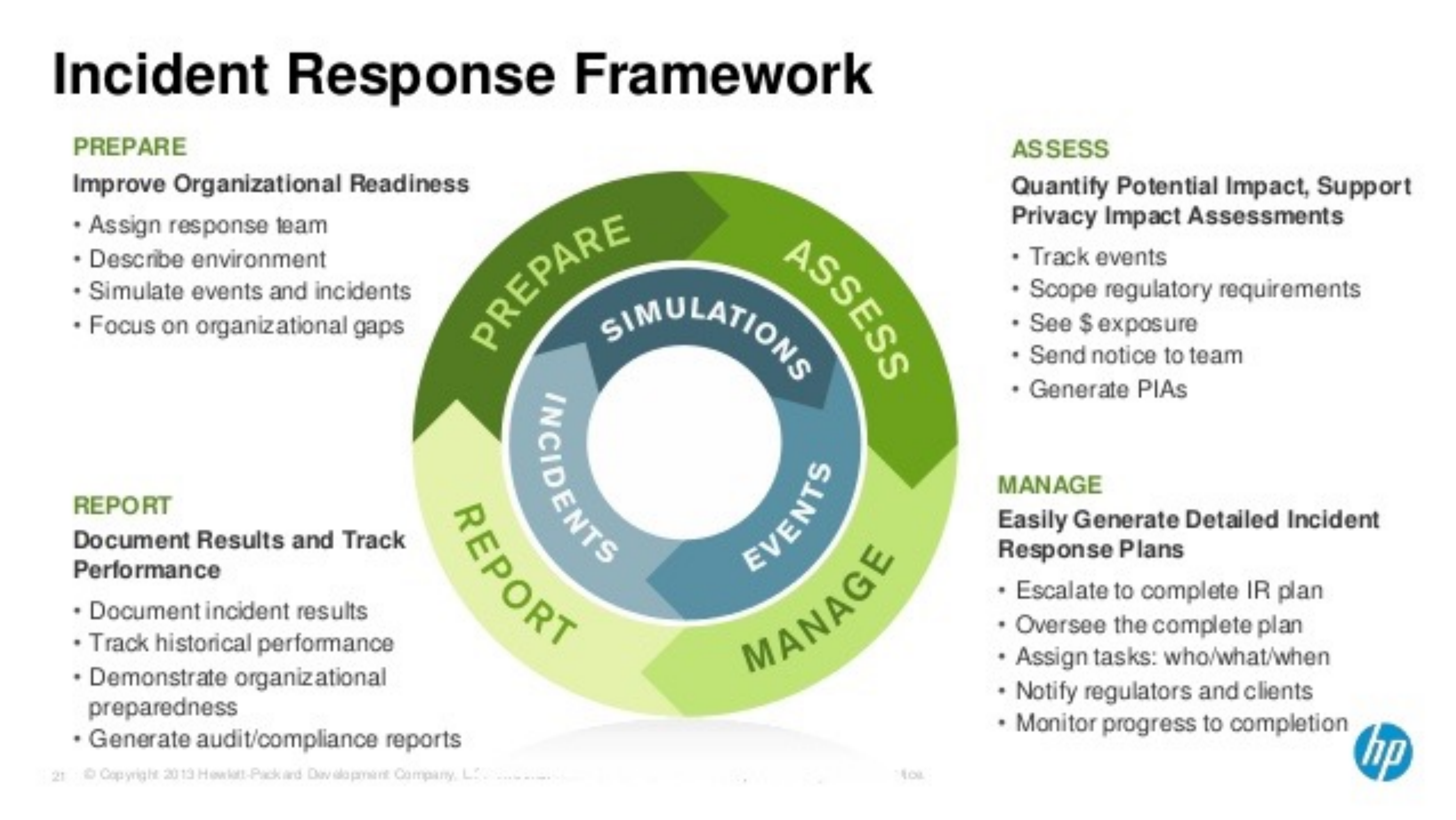
- Network has been under attack for months, gone unnoticed
- Gone unnoticed means that there hasn’t been an IDS/IPS within the network
- As the network has been under attack, the network needs to be hardened
- Both networks don’t communicate securely to each other

NETWORK DESIGN: AFTER



Network to be secured, so that it's harder for attackers to penetrate the network.

INCIDENT RESPONSE FRAMEWORK



Incident Response Framework

PREPARE

Improve Organizational Readiness

- Assign response team
- Describe environment
- Simulate events and incidents
- Focus on organizational gaps

ASSESS

Quantify Potential Impact, Support Privacy Impact Assessments

- Track events
- Scope regulatory requirements
- See $ exposure
- Send notice to team
- Generate PIAs

MANAGE

Easily Generate Detailed Incident Response Plans

- Escalate to complete IR plan
- Oversee the complete plan
- Assign tasks: who/what/when
- Notify regulators and clients
- Monitor progress to completion

REPORT

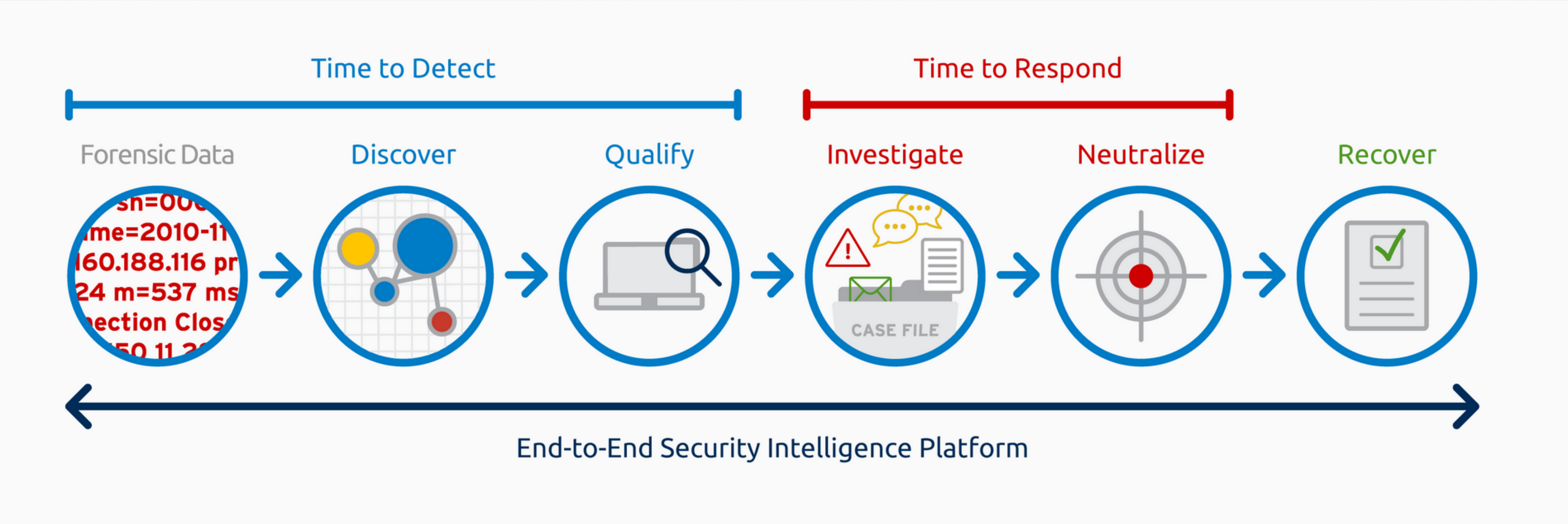
Document Results and Track Performance

- Document incident results
- Track historical performance
- Demonstrate organizational preparedness
- Generate audit/compliance reports

© Copyright 2013 Hewlett-Packard Development Company, L[illegible]tice.

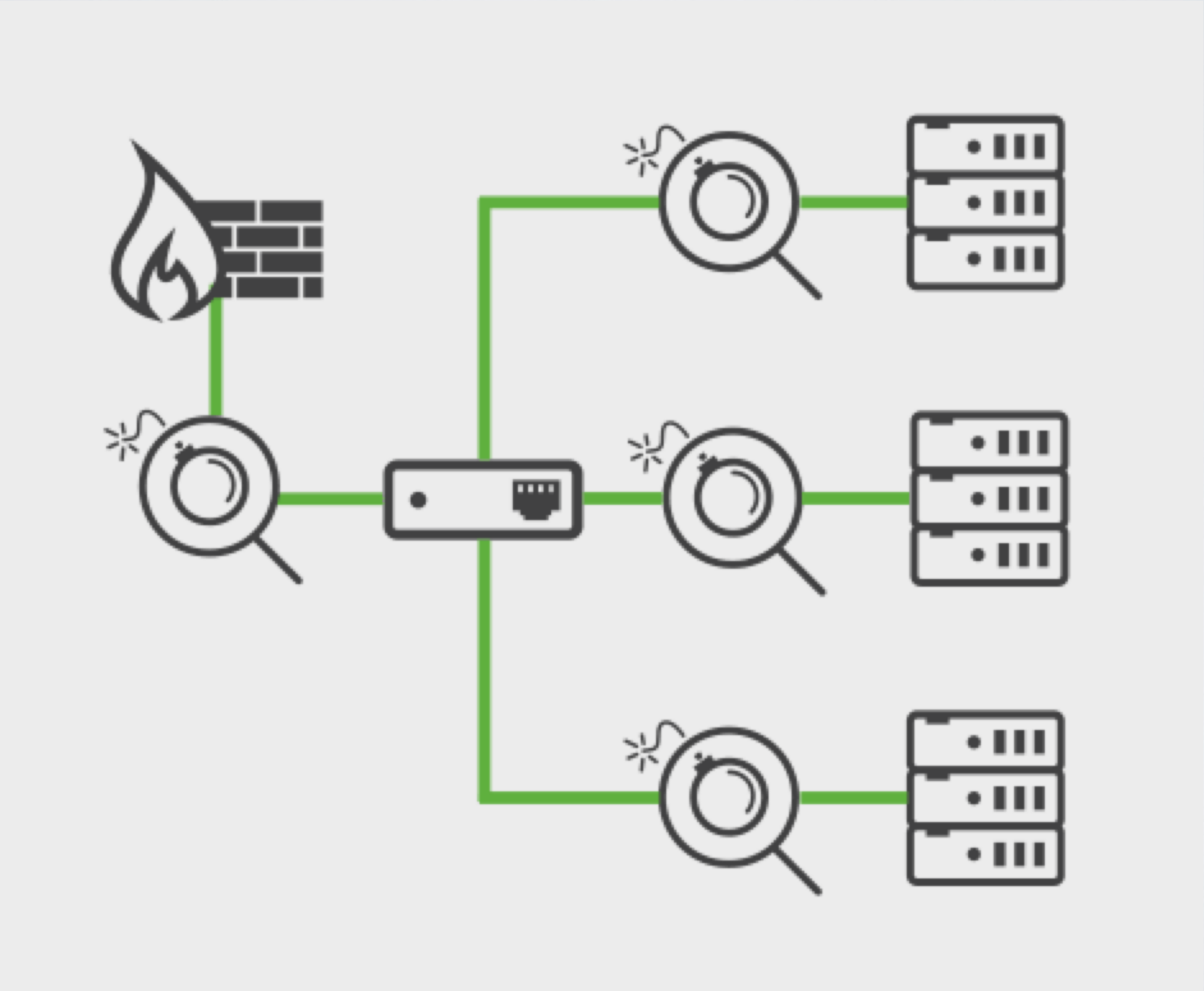
Similar framework to be suggested

THREAT MANAGEMENT SYSTEM

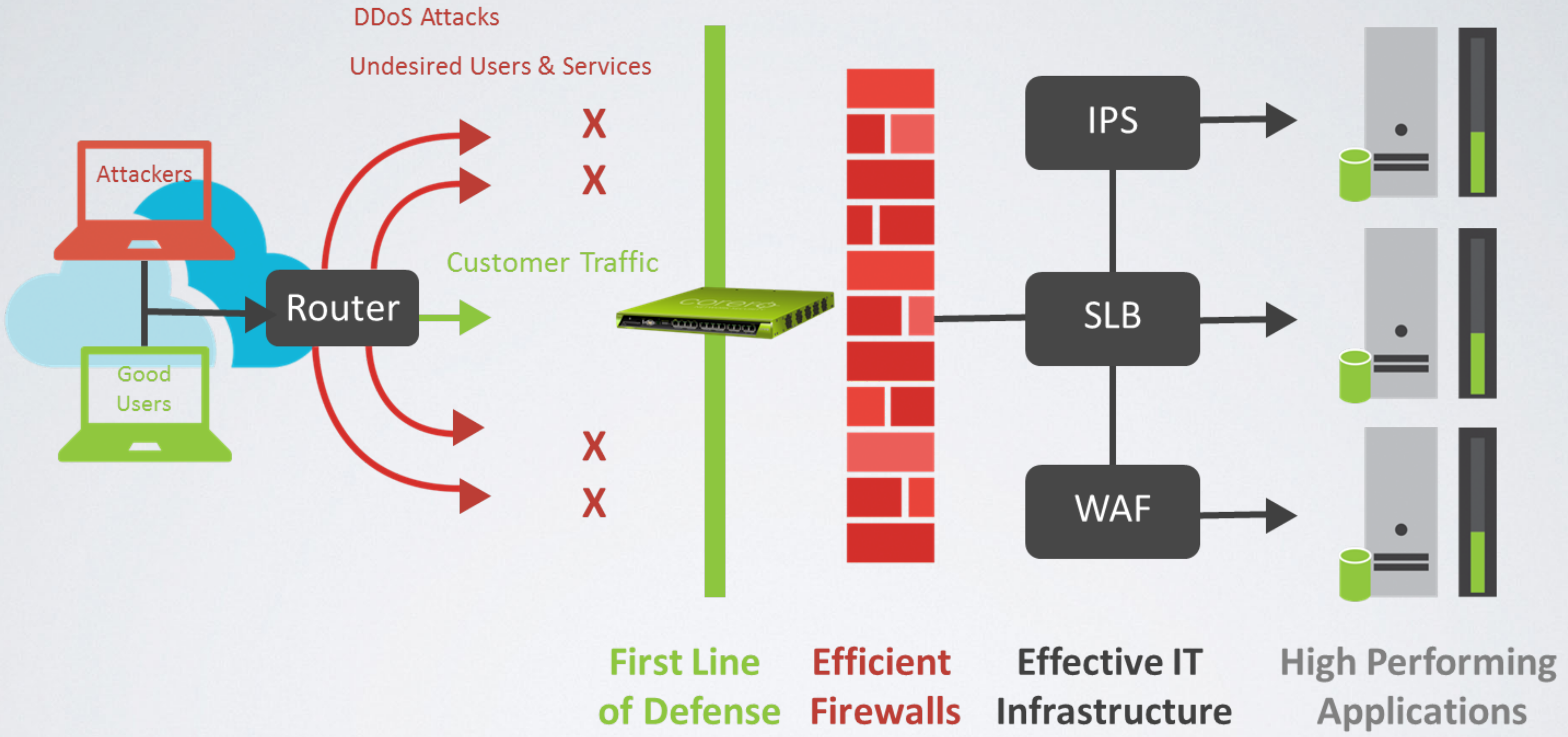


Implement and install a threat management system that detects threats and attacks before it has a chance to infiltrate the system. Or if infiltrated, very quickly discovered and the system to be neutralized.

INTRUSION DETECTION SYSTEM

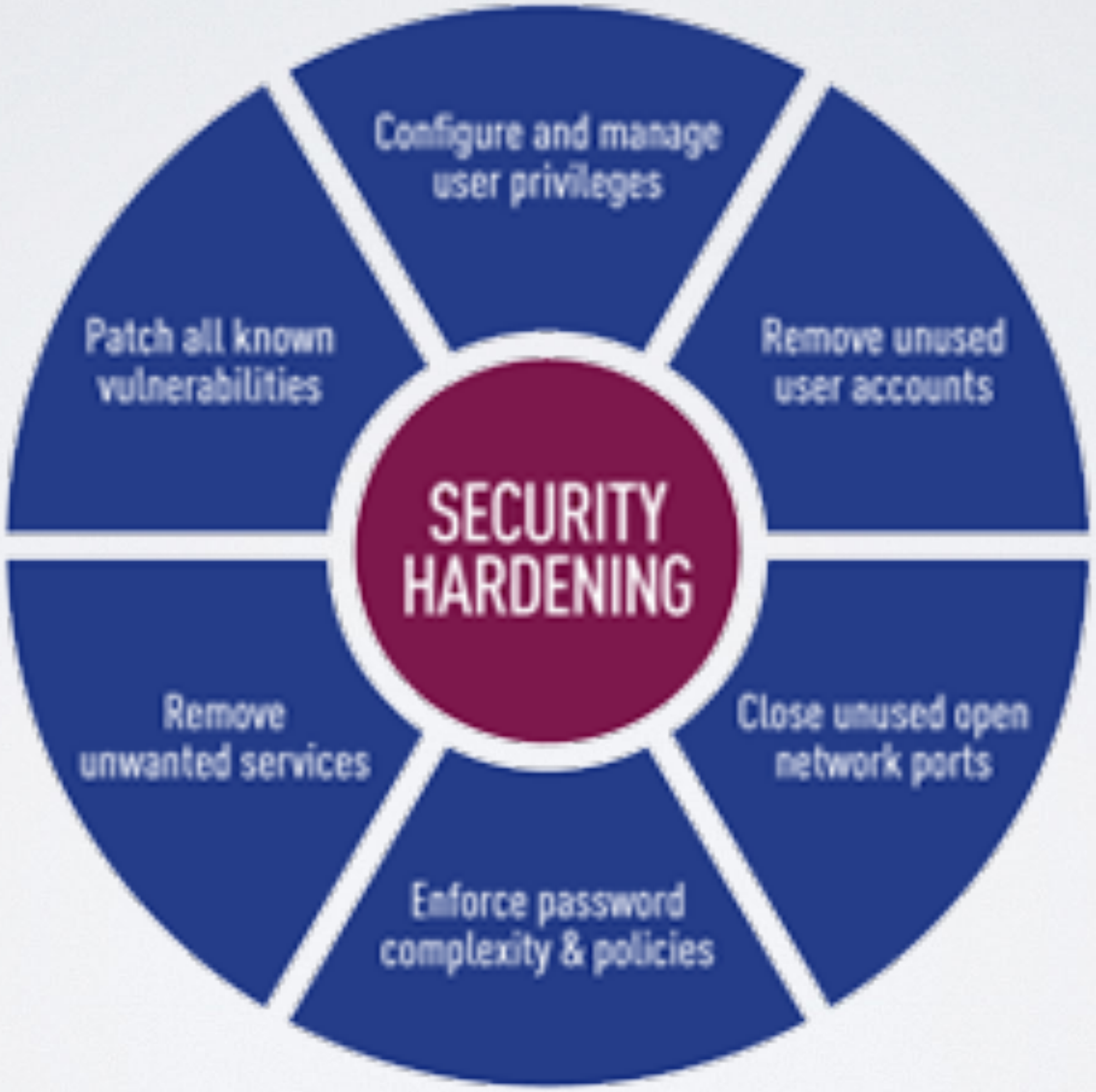


INTRUSION PREVENTION SYSTEM



Similar IPS system to be suggested.

HARDENING OPERATING SYSTEM & WEB SERVER


SECURITY HARDENING
Configure and manage user privileges
Remove unused user accounts
Close unused open network ports
Enforce password complexity & policies
Remove unwanted services
Patch all known vulnerabilities

Similar techniques to be suggested