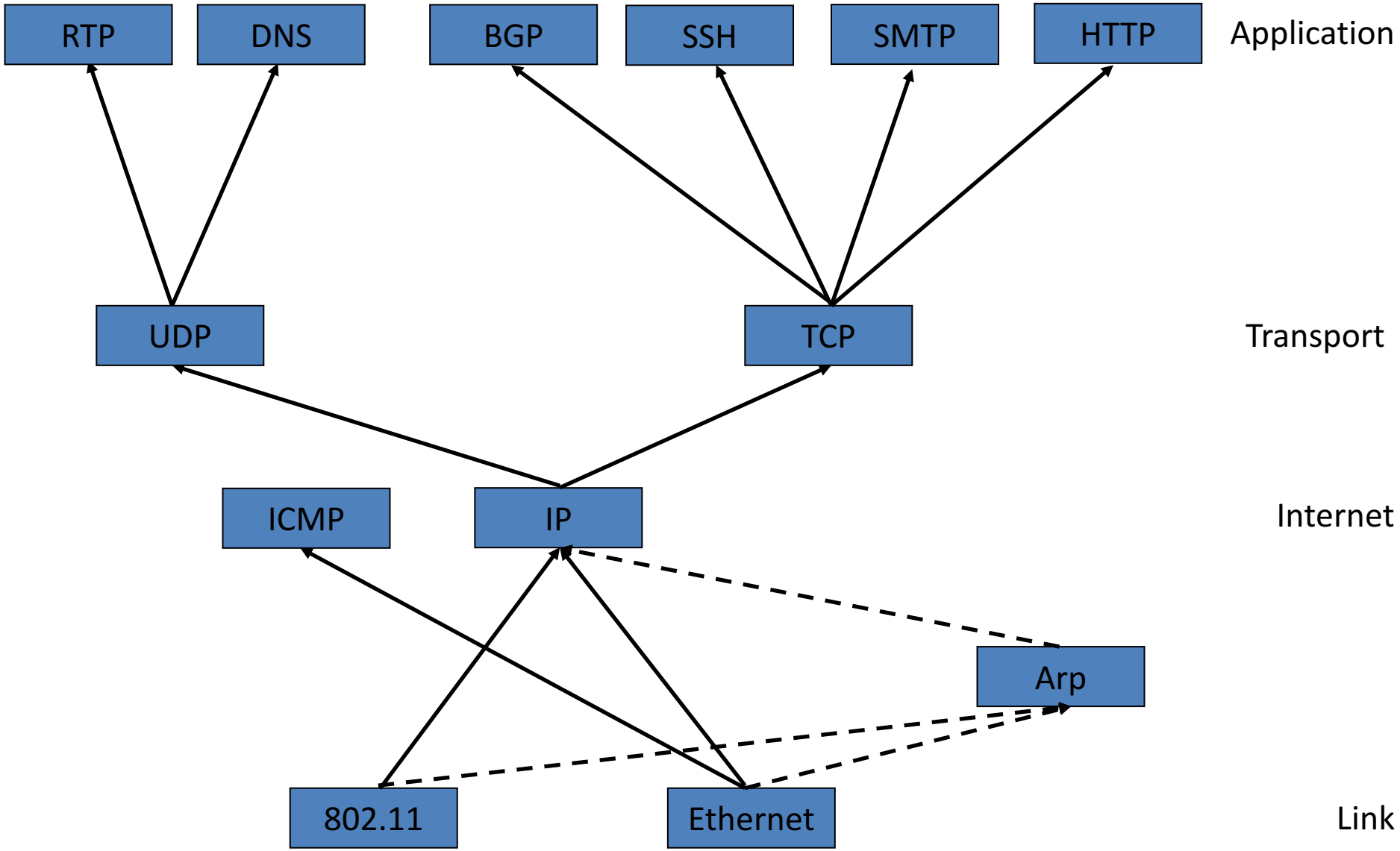
Lecture 25 – Network Defense 2: VPNs & IDS

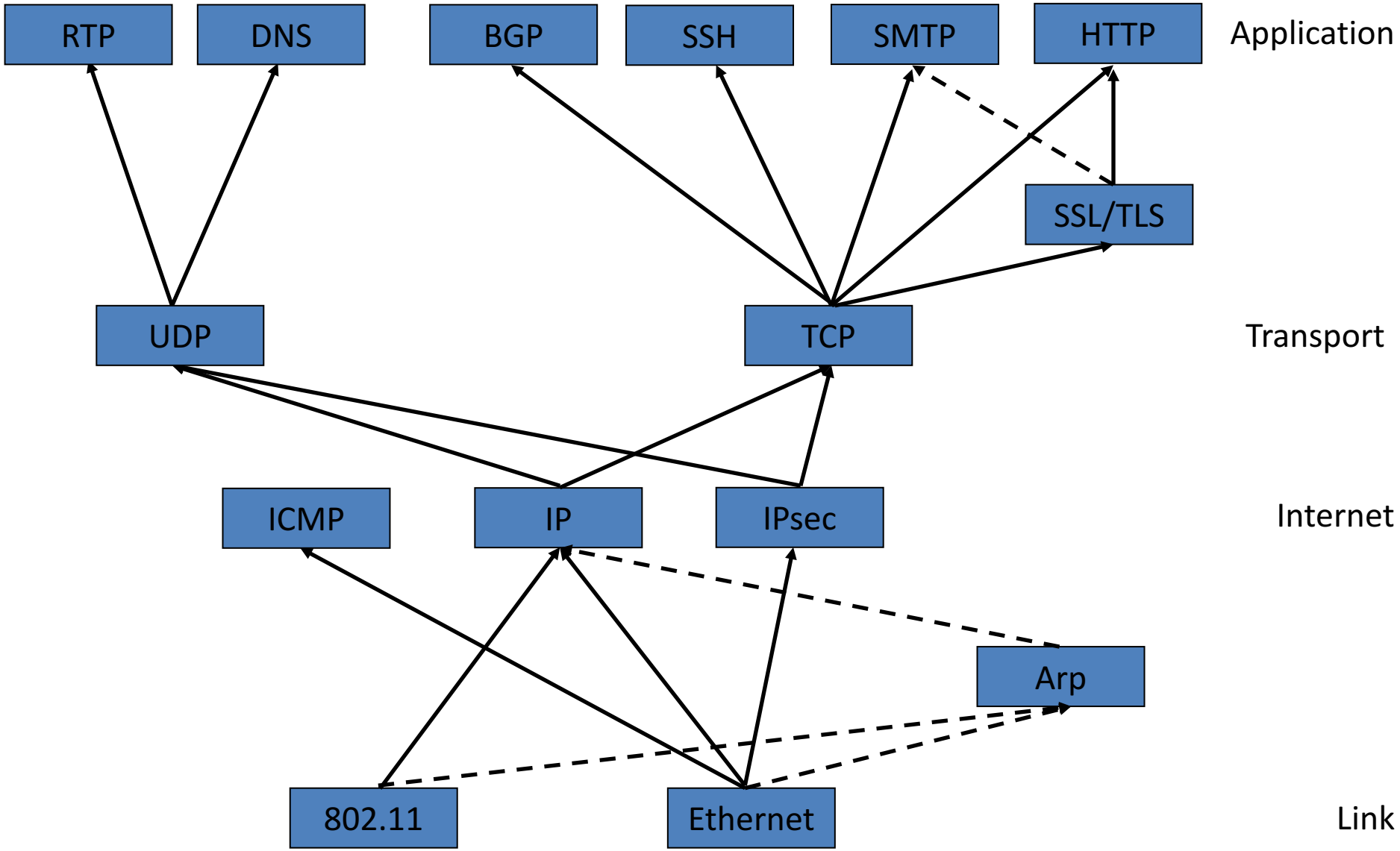
Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017

Security News

- Android adding DNS over TLS
- Stack buffer overflow patched in Chrome
- Equifax was warned of security problems

Secure Protocols & VPNs


RTP
DNS
BGP
SSH
SMTP
HTTP
Application
UDP
TCP
Transport
ICMP
IP
Internet
Arp
802.11
Ethernet
Link


RTP
DNS
BGP
SSH
SMTP
HTTP
Application
SSL/TLS
UDP
TCP
Transport
ICMP
IP
IPsec
Internet
Arp
802.11
Ethernet
Link

SSL/TLS

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (shttp).
- security services:
  - server authentication
  - data encryption
  - client authentication (optional)

- server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Browser requests server certificate, issued by trusted CA.
  - Browser uses CA's public key to extract server's public key from certificate.
- check your browser's security menu to see its trusted CAs.

SSL/TLS (continued)

Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
  - All data sent into TCP socket (by client or server) encrypted with session key.

- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

IPsec: Network Layer Security

- Network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages
- Network-layer authentication
  - destination host can authenticate source IP address
- Two principle protocols:
  - authentication header (AH) protocol
  - encapsulation security payload (ESP) protocol

- For both AH and ESP, source, destination handshake:
  - create network-layer logical channel called a security association (SA)
- Each SA is unidirectional
- Uniquely determined by:
  - security protocol (AH or ESP)
  - source IP address
  - 32-bit connection ID

IPSec Applications

- Establish secure network over internet (e.g. VPN)
  - Remote access, e-commerce
- Transparent to application layer
- Can be implemented by routers
  - Protect user data without their even knowing
- Also secures routing itself
  - Routers themselves are authorized

Authentication Header (AH) Protocol

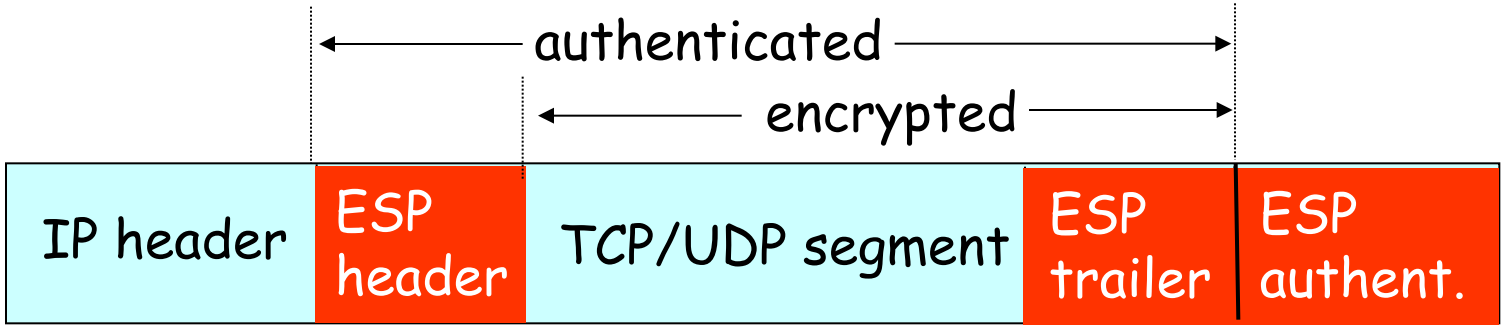
- provides source authentication, data integrity, no confidentiality
- AH header inserted between IP header & data field
- protocol field: 51
- intermediate routers process datagrams as usual

AH header includes:

- connection identifier
- authentication data: source-signed message digest calculated over original IP datagram
- next header field: specifies type of data (e.g., TCP, UDP, ICMP)

ESP Protocol

- provides secrecy, host authentication, data integrity
- data, ESP trailer encrypted
- next header field is in ESP trailer
- ESP authentication field is similar to AH authentication field
- Protocol = 50.



Transport vs. Tunneling

- Two IPSec modes of operation:

1. Transport: encrypt/authenticate payload only
2. Tunneling: wrap entire IP packet in new IPsec packet

- Tunneling allows for NAT & VPNs

Virtual Private Networks

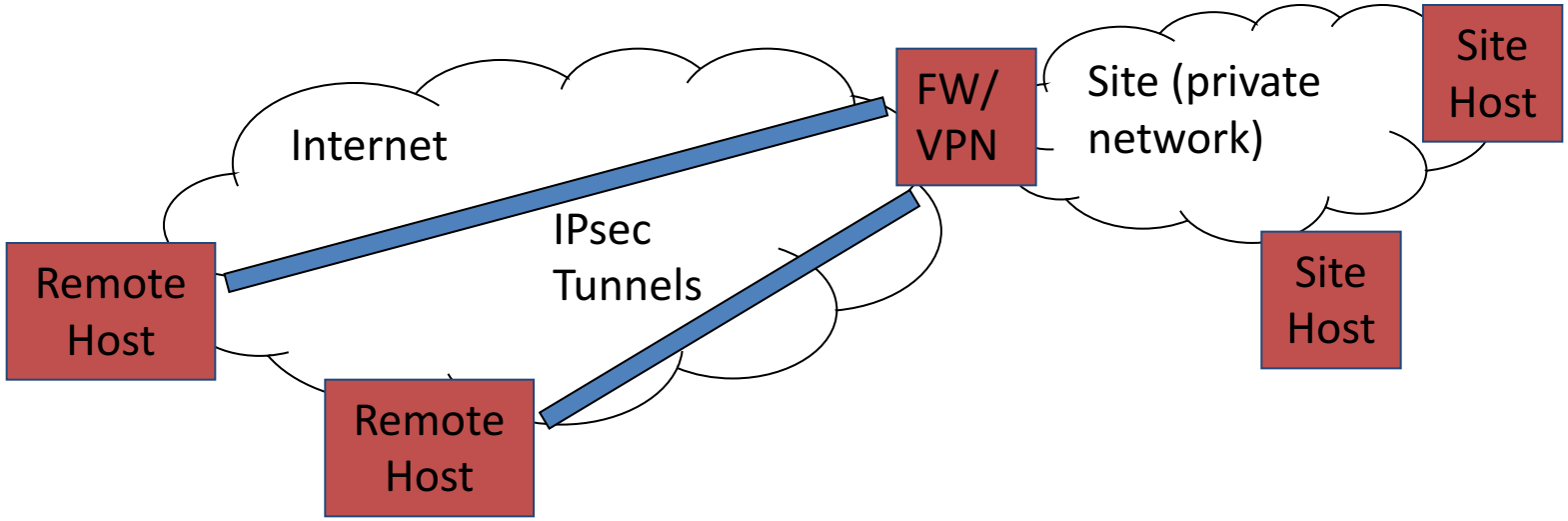
- Setting up a private network over a public connection
  - i.e. over the internet
- Secure communication with IPSec or SSL
  - Authentication
  - Confidentiality
- Can be implemented in or behind a firewall

IP VPN benefits

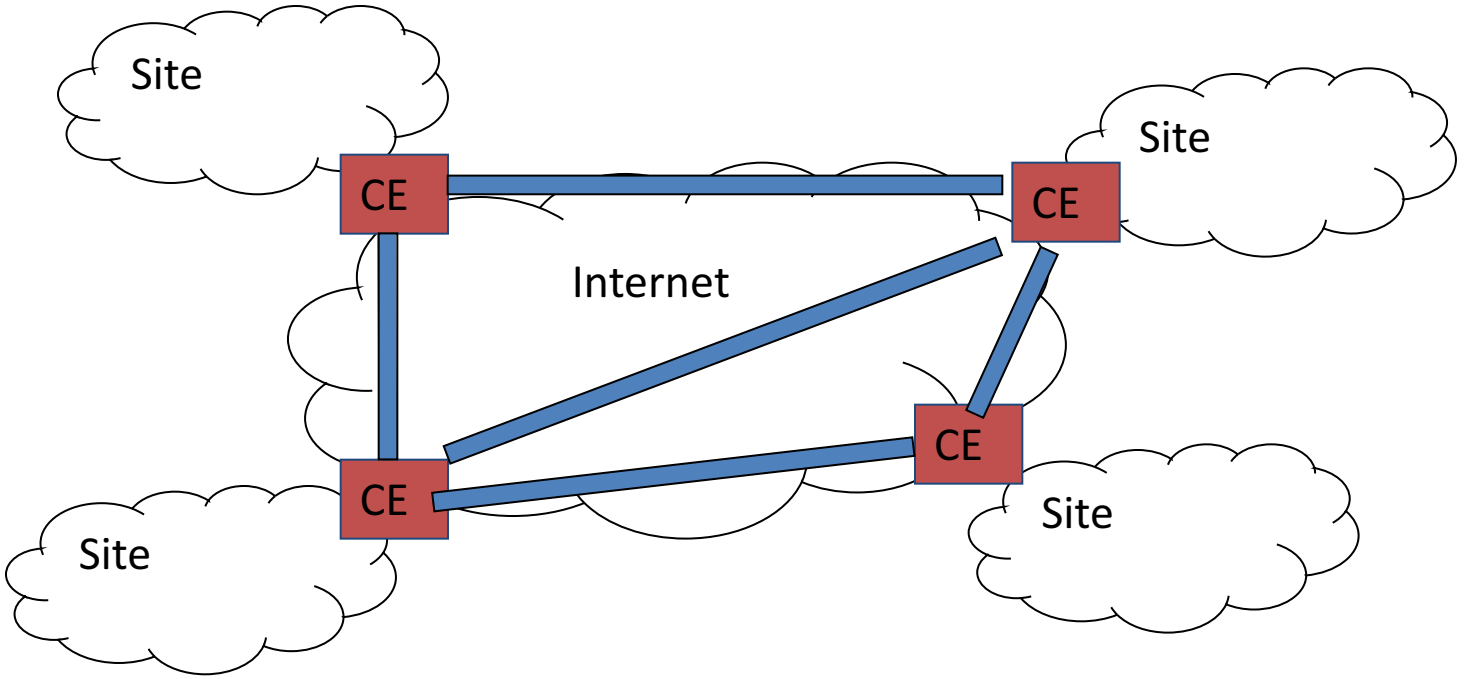
- IP not really global (private addresses)
  - VPN makes separated IP sites look like one private IP network
- Security
- Bandwidth guarantees across ISP
  - QoS, SLAs
- Simplified network operation
  - ISP can do the routing for you

End-to-end VPNs

- Solves problem of how to connect remote hosts to a firewalled network

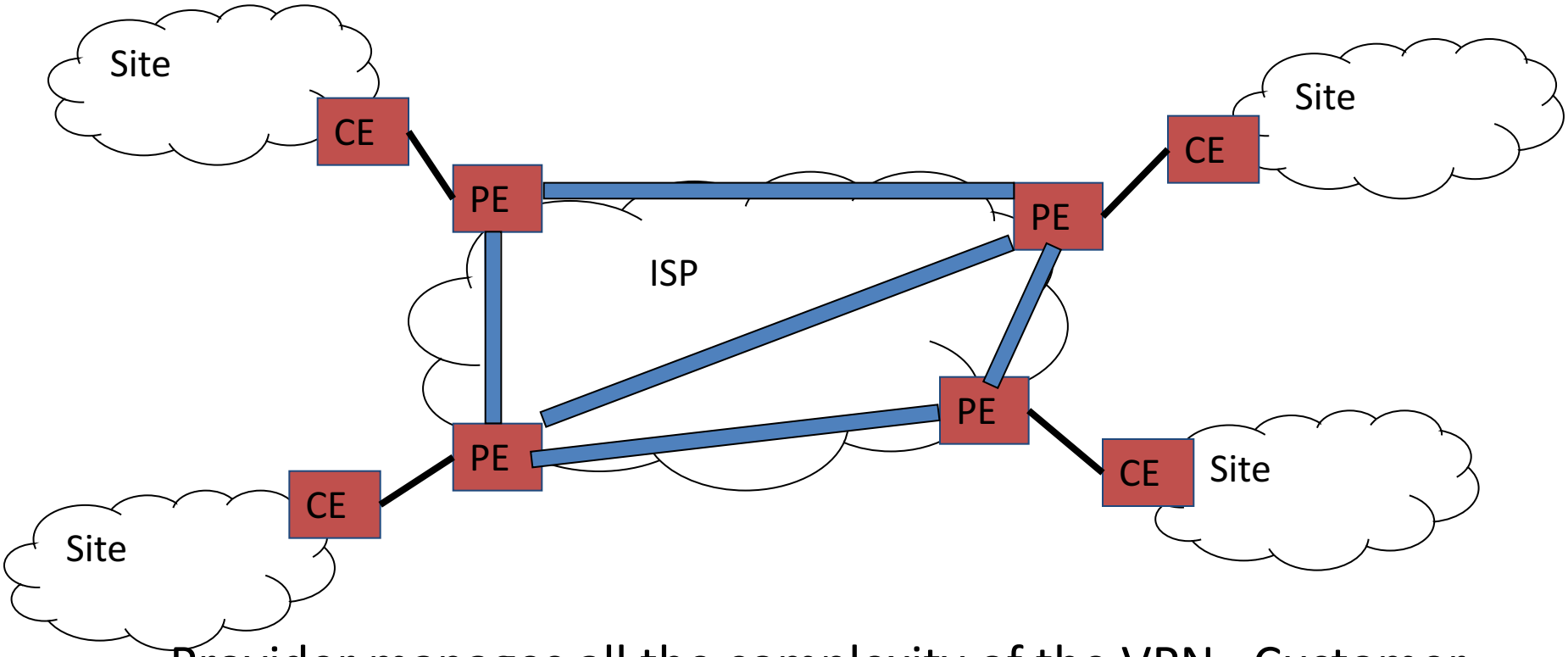


Customer-based Network VPNs



Customer buys own equipment, configures IPsec tunnels over the global internet, manages addressing and routing. ISP plays no role.

Provider-based Network VPNs



Provider manages all the complexity of the VPN. Customer simply connects to the provider equipment.

NETWORK BASED IDS

Intrusion detection

- “Building burglar alarms for the net”
- Idea: make systems sensitive to threatening actions, and make them capable of alerting authorities when they notice anomalies
- Necessarily post-hoc
- Broad types
  - Statistical analyzers (anomaly based)
  - Rules-based systems, Attack-signature detectors (misuse)
  - Others

Intruder Behavior

1. Target acquisition and information gathering
   - Map network, identify vulnerable services, social engineering
2. Initial access
   - Brute force user's web based password, exploit remote vulnerability, spear-phish browser exploit
3. Privilege escalation
   - Exploit local application with elevated privileges, capture admin password

Intruder Behavior

4. Gather information or exploit system
   - Scan for other targets or capture sensitive data
5. Maintaining access
   - Install rootkit backdoor, disable anti-virus/IDS
6. Covering tracks
   - Modify logs and remove any trace of intrusion, use rootkit to hide files installed on the system

Know Your Attacker

- Most attackers run scripts to probe for vulnerabilities, then return later to exploit them
- Probes tend to come in waves as new holes are discovered
- Probes look very different than typical network use
- Actual attack may come long after probe

Paradigms in Intrusion Detection

- **Misuse Detection Intrusion Detection Systems (MD)**
  - define *"what is abnormal"* using attack signatures
  - traffic that matches an attack signature as attack traffic
- **Anomaly Detection Intrusion Detection Systems (AD)**
  - define *"what is normal"* using profiles
  - traffic that does not match the profile as abnormal

The world's simplest IDS

```
v=listen(frequently-exploited-unused-port);
while(1) {
    s=accept(v, who, howbig);
    notify_the_authorities(s, who, howbig);
    close(s);
}
```

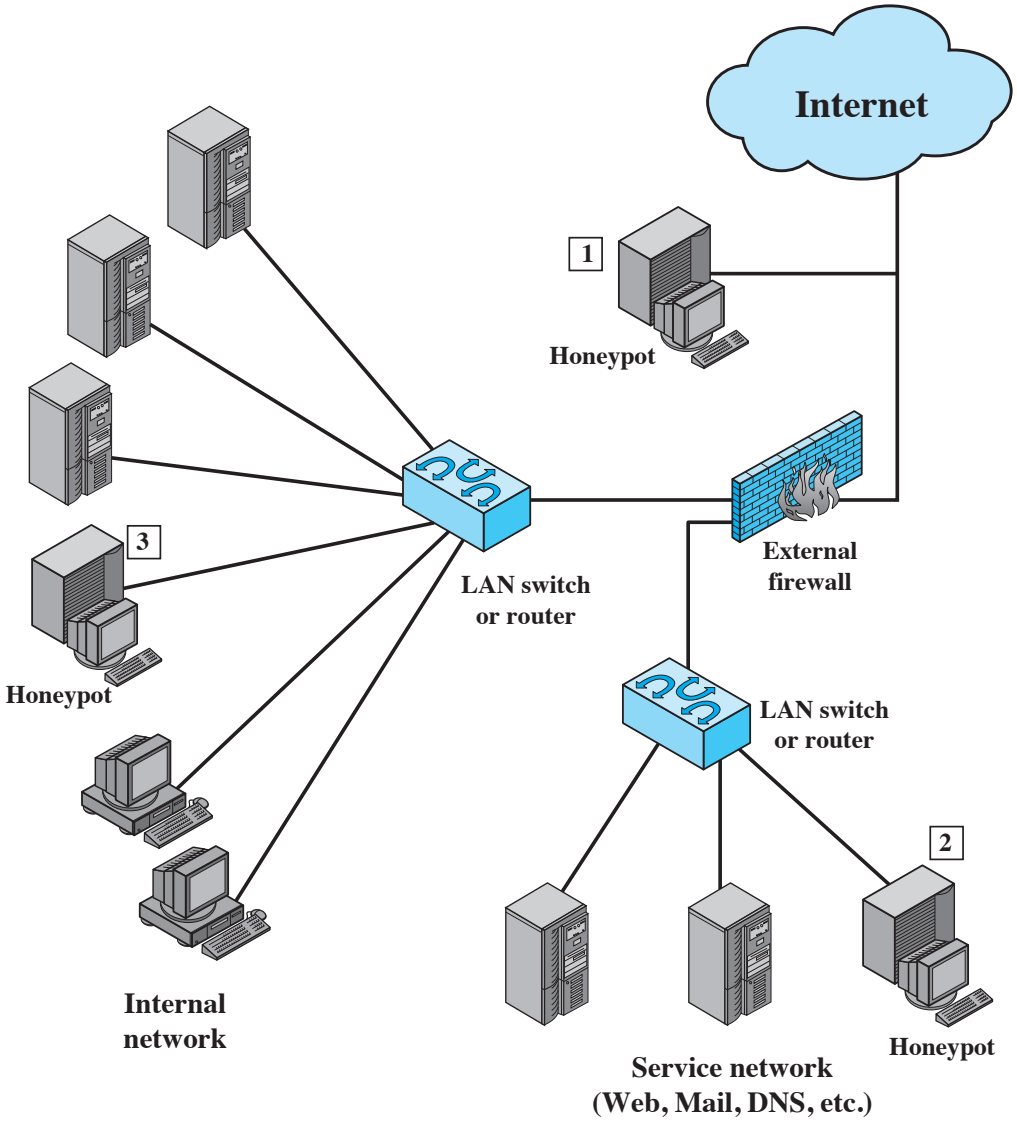
- This won't catch stealth scanners
- Doesn't have a global view
- Can't detect attacks on systems in use
- Surprisingly effective at catching scans nonetheless

Honeypots

- Decoy systems designed to
  - Divert attacker from critical systems
  - Collect information about attacker's activity
  - Encourage attacker to remain on system so administrators can respond
- Two kinds:
  - Low interaction honeypot - Emulates particular IT service
  - High interaction honeypot - real system with full OS

http://en.wikipedia.org/wiki/Winnie-the-Pooh

Honeypot Deployment



Statistical analysis

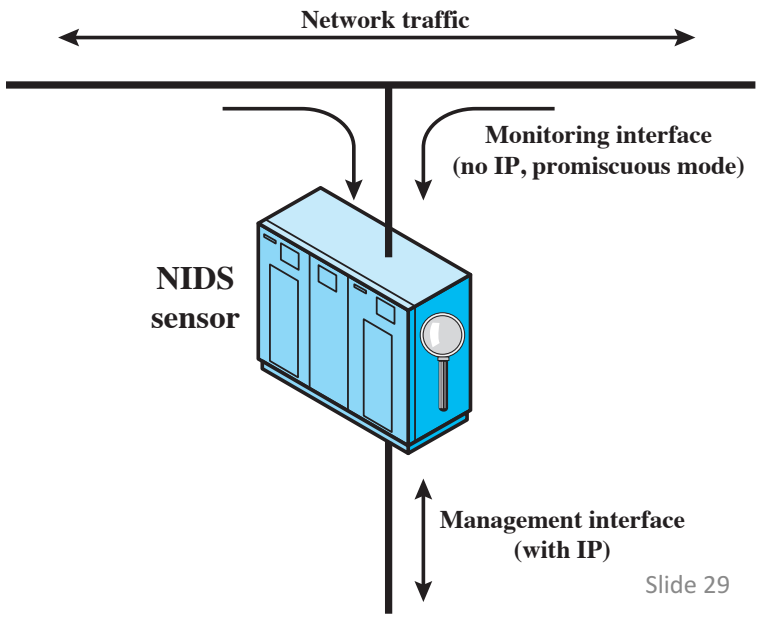
- Constantly capture packets, watch logs, note typical flows
  - I.E. “95% of traffic flows from inside the firewall to outside web services”
  - Set off alarm bells when traffic not matching typical flows is seen
  - Can be a first alert against configuration problems
- Gains a global picture of the system

Rule-based systems

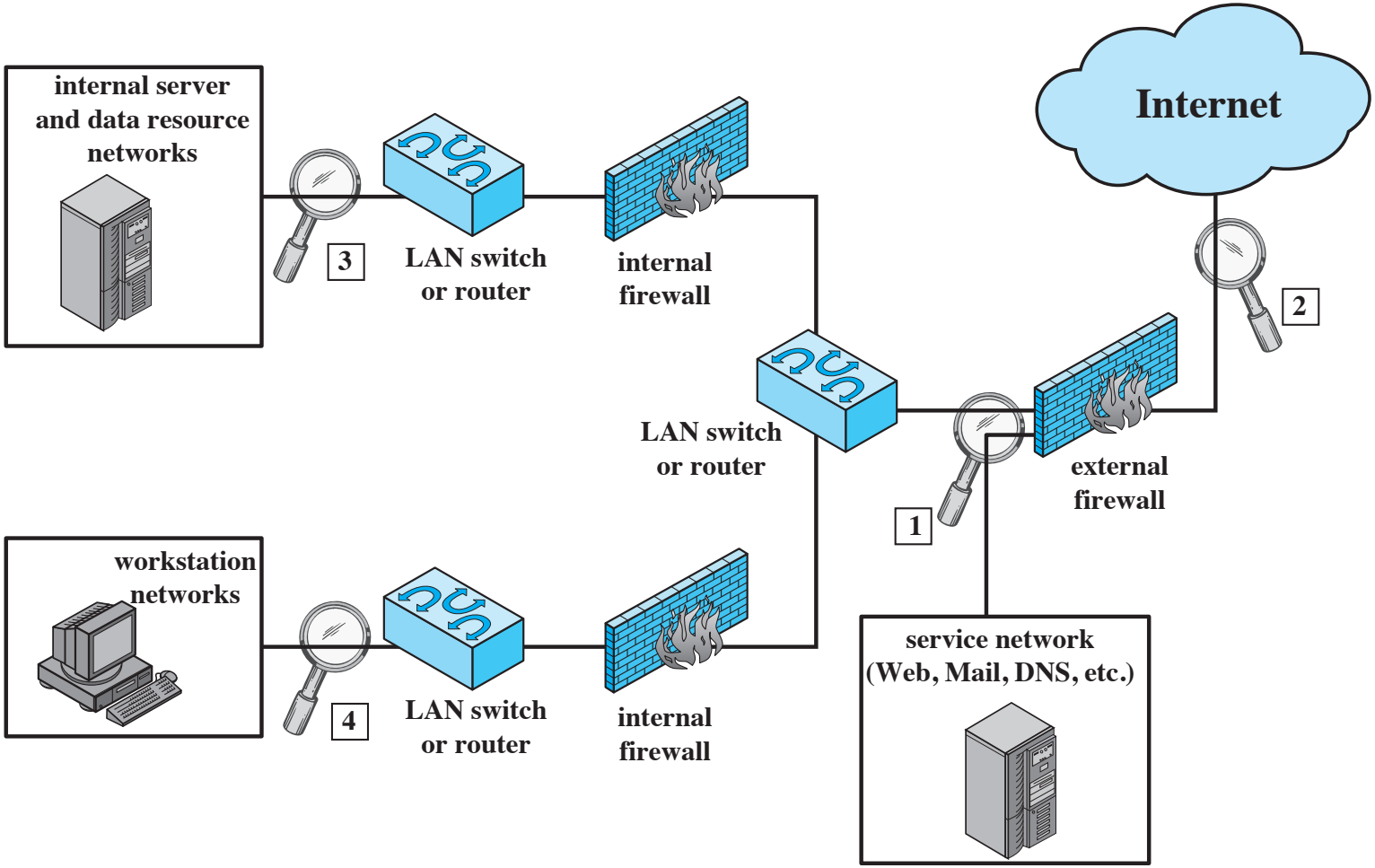
- Monitor logs and network for behavior violating or matching static rules
- Require some knowledge of attack behaviors
- Less prone to false alarms
- Often combined with anomaly detectors

Network-Based IDS (NIDS) Sensors

- Inline sensor
  - Monitored traffic passes through the sensor
  - Can be combined with firewall or switch
- Passive sensor
  - Monitors a ***copy*** of network traffic

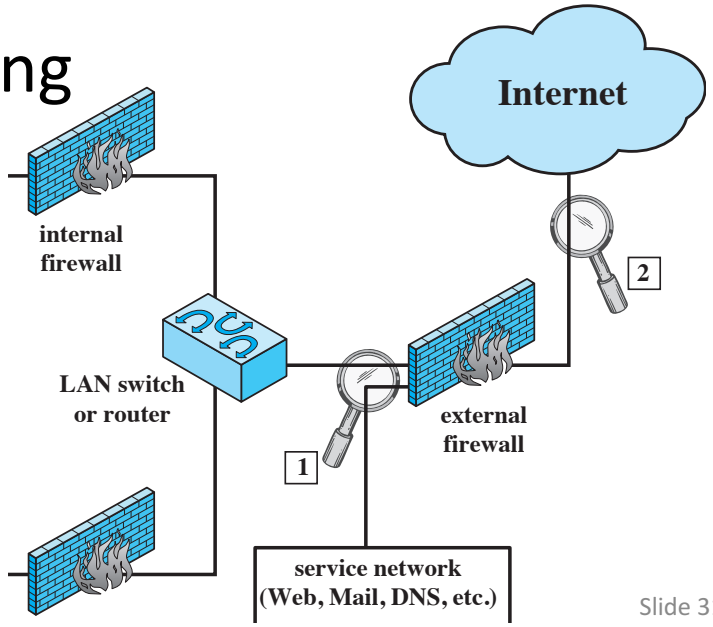


Network-Based IDS (NIDS) Sensors



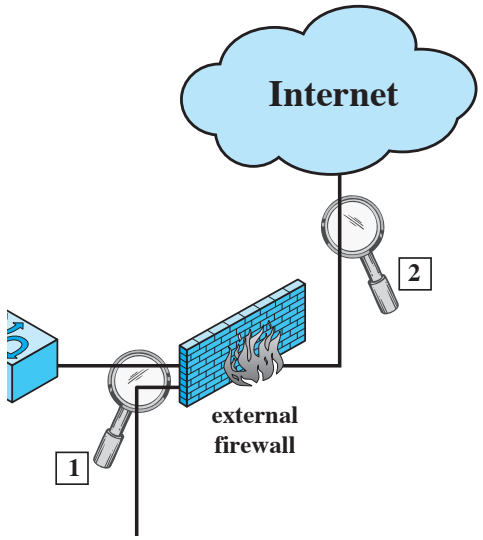
Network-Based IDS (NIDS) Sensors

- 1) Inside the firewall
  - See attacks from outside that pass firewall
  - Can identify firewall configuration problems
  - Can detect attacks against web/ftp server
  - Can perform egress monitoring
  - Can't detect attacks inside network



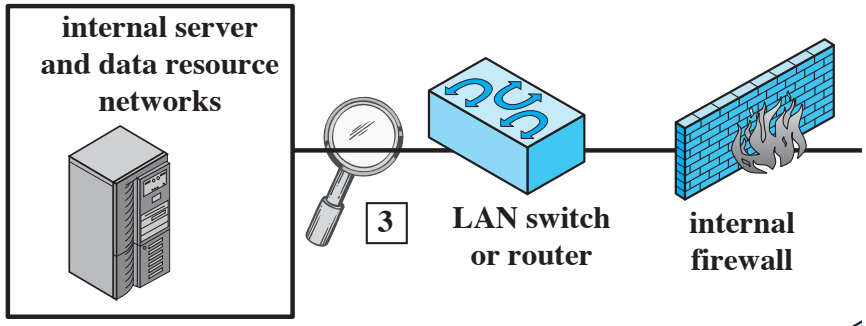
Network-Based IDS (NIDS) Sensors

- 2) Outside the firewall
  - See *all* attacks targeting your network
  - Much higher processing burden (backscatter, Blaster Worm)



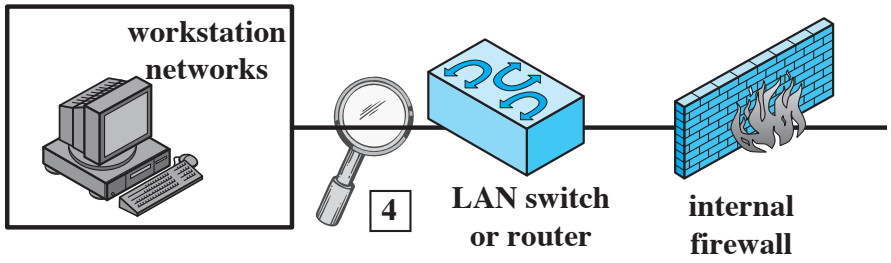
Network-Based IDS (NIDS) Sensors

- 3) Major internal backbone networks
  - Internal servers/databases
  - View a large amount of internal network traffic
  - Detect unauthorized activity within security perimeter
  - Can monitor specific protocols and attack types



Network-Based IDS (NIDS) Sensors

- 4) Workstation LANs
  - Can target specific subnetworks
  - Focus limited resources on important assets
  - Detect unauthorized activity within security perimeter
  - Can monitor specific protocols and attack types



NIDS Signature Detection

- Application layer reconnaissance/attacks
  - Look for known attack patterns in specific protocols
  - e.g. DHCP, IMAP, IRC, NFS, POP, SMTP, Telnet
  - Find buffer overflow, password guessing, malware transmission
- Transport layer reconnaissance/attacks
  - Look at TCP/UDP traffic to identify known attacks
  - Port scans, packet fragmentation, SYN floods
- Network layer reconnaissance/attacks
  - Look at IP, ICMP for spoofed IP addresses/illegal IP headers

NIDS Signature Detection

- Unexpected application services
  - Look for traffic that indicates an unwanted application
  - IRC/chat clients common for botnets
  - TOR/BitTorrent traffic might not be a good sign
- Policy violations
  - Look for inappropriate website visits
  - Video game/social network use

NIDS Anomaly Detection

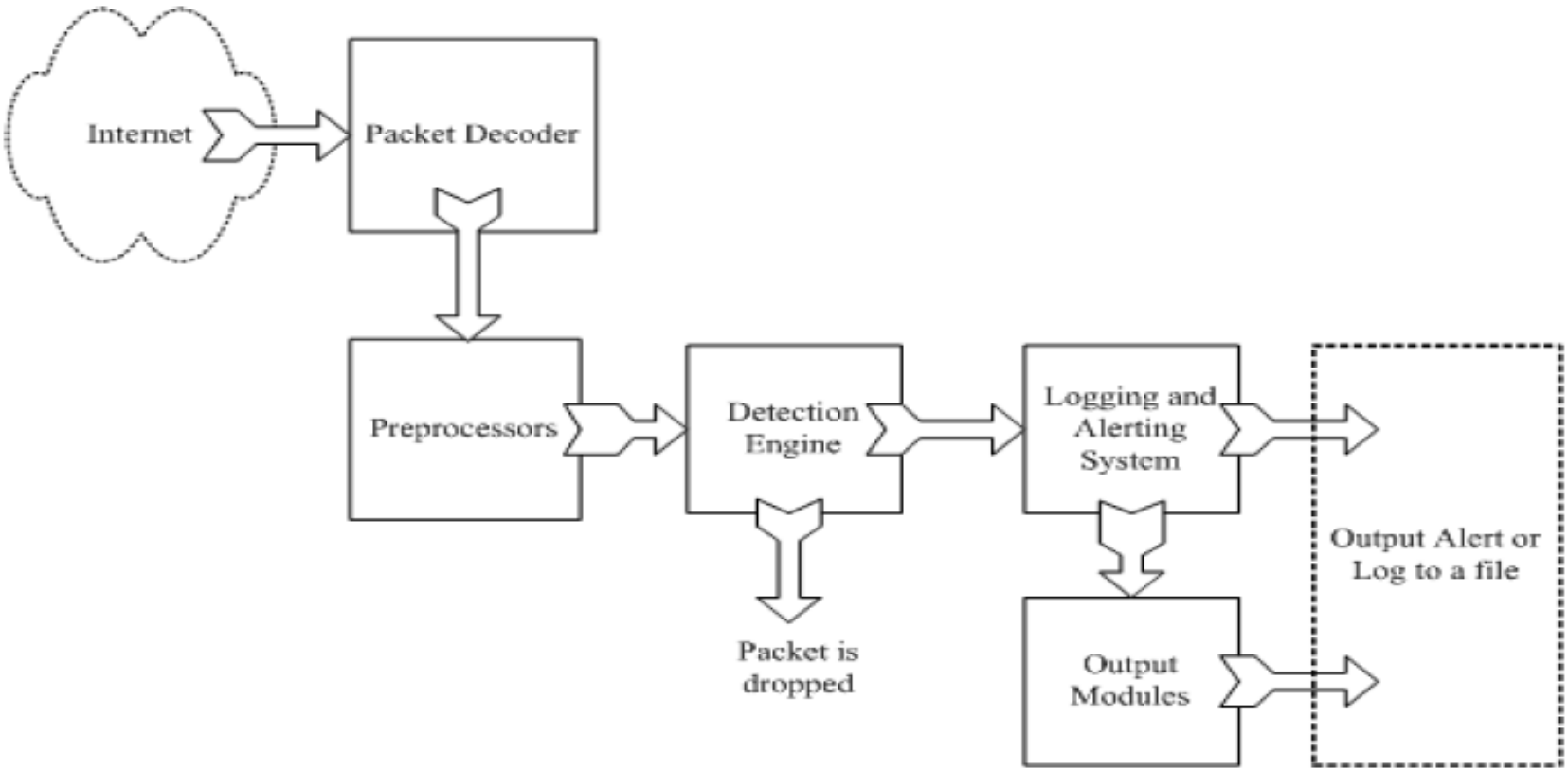
- DoS attacks
  - Look for increased traffic/connection attempts
- Scanning
  - Look for atypical flow patterns at application layer, transport layer, or network layer
- Worms
  - Look for hosts communicating that typically don't
  - Look for ports used that typically arent

NIDS Stateful Protocol Analysis (SPA)

- NIDS can also be used to observe state of connections
- Make sure they proceed as normal
- SPA has a high resource cost

Example: Snort

http://www.snort.org/

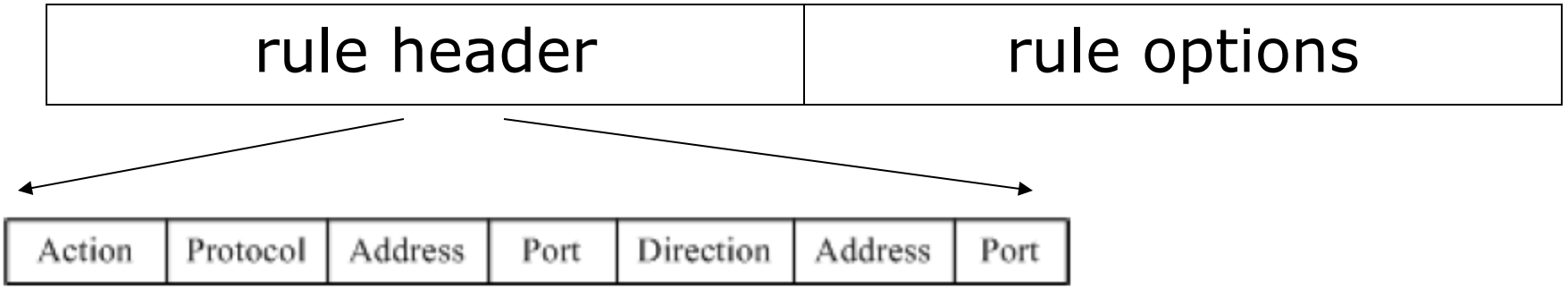


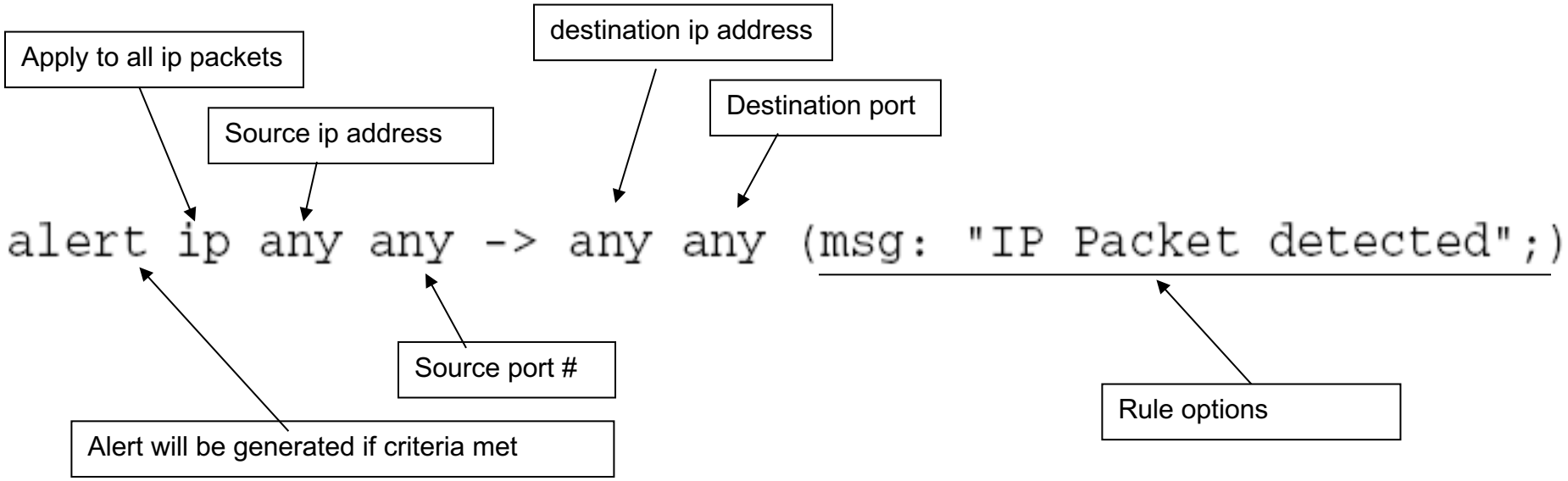
From: Rafeeq Ur Rehman, *Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID.*

Snort components

- Packet Decoder
  - input from Ethernet, SLIP, PPP…
- Preprocessor:
  - detect anomalies in packet headers
  - packet defragmentation
  - decode HTTP URI
  - reassemble TCP streams
- Detection Engine: applies rules to packets
- Logging and Alerting System
- Output Modules: alerts, log, other output

Snort detection rules





Additional examples

alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd access";)

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111
(content: "|00 01 86 a5|"; msg: "external mountd access";)

! = negation operator in address

content - match content in packet

192.168.1.0/24 - addr from 192.168.1.1 to 192.168.1.255

https://www.snort.org/documents/snort-users-manual

Using an IDS

- Plan your incident response process well before you install the system
- Know what you're looking for
- Make the system comprehensive
- Don't overreact to alarms
- If using a rules-based system, keep up with vulnerability reports