CPSC 317
COMPUTER NETWORKING

Module 8: Security – Day 5 – IPSec, VPN, Firewall, IDS

Some slides based on Kurose/Ross original slides, found at https://gaia.cs.umass.edu/kurose_ross/ppt.htm

ADMINISTRATION

- Quiz 5 wraps up today
- Student Experience of Instruction surveys open now until April 15th
- Survey for last lecture closes tomorrow
  - 84 responses – please all fill SEI survey
  - Every topic is difficult (?!)
- No clickers today

LEARNING GOALS

- Describe how IPsec provides all the elements of a security protocol
- Describe the problem that a VPN addresses
- Explain what a tunnel is, and how it works
- Describe the role that a firewall plays, and how it works
- Explain the difference between stateless and stateful packet filters
- Explain what an application gateway does
- Explain what an Intrusion Detection System (or Intrusion Prevention System) does

READING

- Reading: 8.7

NETWORK LAYER SECURITY: IPSEC

- IPsec provides datagram-level encryption, authentication, integrity
  - For both user traffic and control traffic (e.g., BGP, DNS, ICMP)
- Can be used to implement a VPN
  - Though there are alternatives using protocols like TLS

IPSEC SUMMARY

- IPsec peers can be end systems, routers, firewalls, or a mix of these
- Association can be done manually or using protocols like IKE (Internet Key Exchange)
  - Policies, algorithms, secret keys, identification
- Provides source authentication, integrity and confidentiality

IPSEC PACKET FORMAT

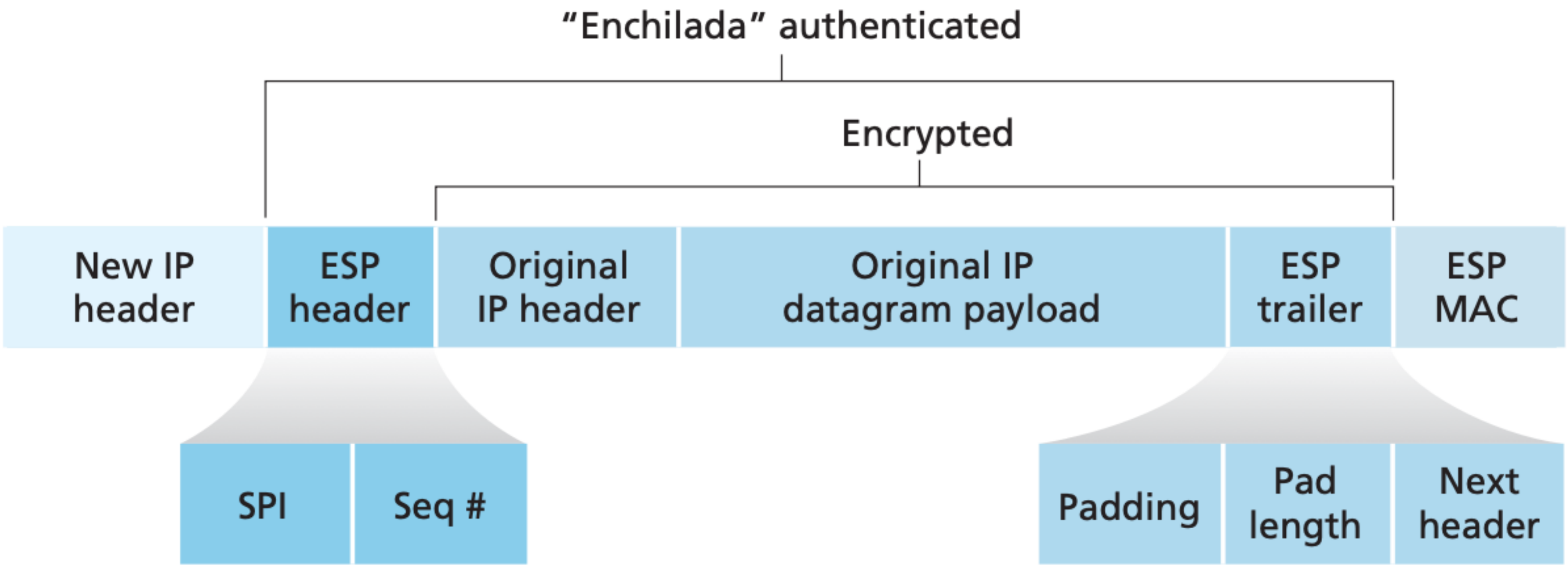


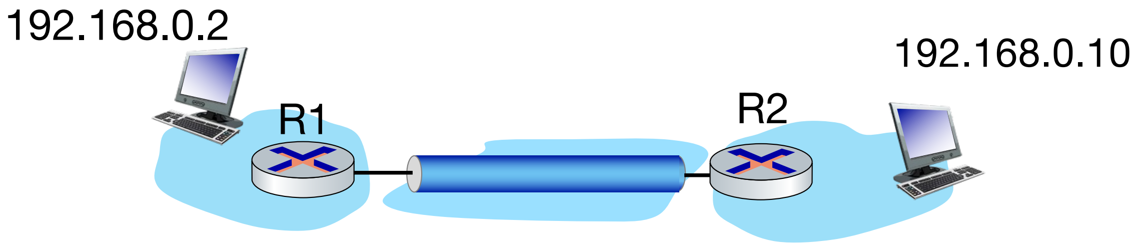
Figure 8.29 ♦ IPsec datagram format

VIRTUAL PRIVATE NETWORK (VPN)

- Motivation
  - Company with multiple locations wants everything to appear as one big network
  - Workers want access to resources restricted to company internal network (e.g., hardware, restricted content, etc.)
  - Students want access to restricted material inside UBC network
  - Users want to bypass regional blocks (e.g., Netflix)

VIRTUAL PRIVATE NETWORK (VPN)

- Solution: pretend you are somewhere else
- Virtual network interface cards on two end point systems

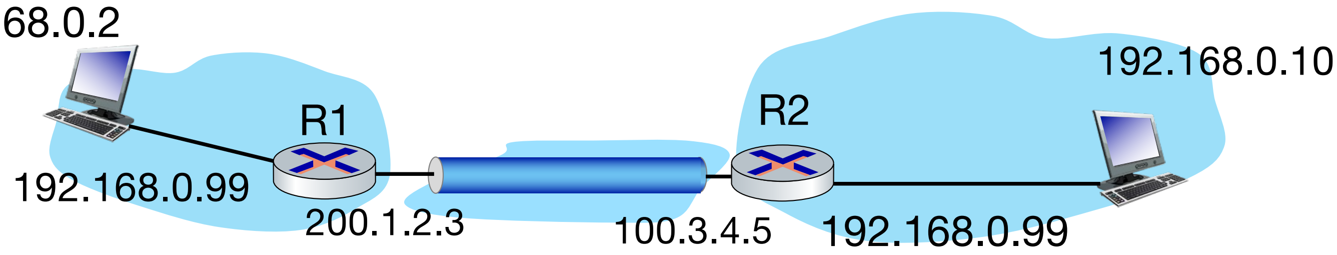


VPN ENCAPSULATION

- Virtual end points establish a software association between them
  - e.g., a TCP connection or IPsec association or TLS connection
  - This is called a tunnel
- Routing rules send traffic to virtual card
- Virtual card encapsulates IP message and sends it into the virtual connection
- Receiver receives this IP message and sends it through its own network

VPN EXAMPLE

Src IP: 192.168.0.2 Dst IP: 192.168.0.10	Src Port: 12345 Dst Port: 515	Payload



Src IP: 200.1.2.3 Dst IP: 100.3.4.5	Src Port: 4832 Dst Port: 1044	VPN Payload (Encapsulated packet)

VPNS CAN ALSO PROVIDE PRIVACY

- The payload that flows through the VPN tunnel can be encrypted so no one can see the contents

TUNNELING MORE GENERALLY

- IPv4 / IPv6
- SSH tunneling
  - Run GUI application on a remote server
  - Access a remote file system as if it were local
- Bypass firewalls (more later)
- There are a number of general purpose tunneling protocols
  - IPsec – IP Secure
  - GRE - Generic Routing Encapsulation
  - TLS – Transport Layer Security
    - Derived from SSL – Secure Socket Layer

SECURITY IN OTHER PROTOCOLS

- DNS → DNSSEC (RFC 4033, 4034, 4035)
- BGP → BGPSec (RFC 8205)
- E-mail → PGP (OpenPGP: RFC 4880)

SECURITY IN OTHER PROTOCOLS

- DNS → DNSSEC (RFC 4033, 4034, 4035)
  - Adds authentication for DNS servers
  - Uses PKI (public-key infrastructure aka asymmetric cryptosystem)
  - Each DNS server signs its RRs
  - No confidentiality

SECURITY IN OTHER PROTOCOLS

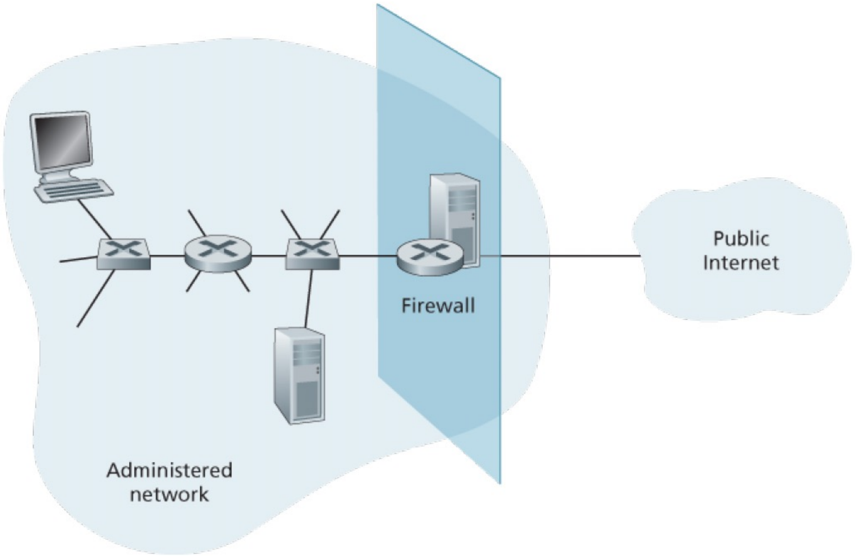
- BGP → BGPSec (RFC 8205)
  - Adds integrity for BGP paths
  - Uses PKI
  - Router adds AS number of the AS it's sending the update to and signs its update
  - No confidentiality

SECURITY IN OTHER PROTOCOLS

- E-mail → PGP (OpenPGP: RFC 4880)
  - Confidentiality, integrity, authentication
  - Every user has a unique public-private key pair
  - One symmetric key for every email (session)
  - Sender encrypts message with session key and the session key with the recipient’s public key

ACCESS AND AVAILABILITY: FIREWALLS

- Operational security (manage availability and access)
- Firewall isolates internal network from public Internet
  - All traffic from outside to inside (or vice-versa) passes through the firewall
  - Allows some datagrams to pass, blocks others
- Typically located in a router



FIREWALLS

- Allow some datagrams to pass, blocks (drops) others
- Based on set of rules (access control lists)
- Used to:
  - Prevent illegal access/modification of internal data
  - Allow only authorized access to inside network
  - Prevent DoS attacks (e.g., SYN flooding)

STATELESS PACKET FILTERING

- Filter packet-by-packet, decision to forward/drop based on:
  - Source/destination IP address and protocol
  - Source/destination TCP/UDP port numbers
  - ICMP message type
  - TCP flags (e.g., SYN/ACK bits)
  - Other header values

STATELESS PACKET FILTERING

- Stateless filtering can be used to:
  - Block inbound TCP segments with ACK=0
  - Block inbound or outbound TCP segments with port=23 (Telnet)
  - Block inbound ICMP messages to broadcast IP address
  - Block outbound ICMP expired TTL messages
    - traceroute uses such ICMP messages

ACCESS CONTROL LISTS

- ACL: table of rules, applied in order to incoming packets:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

STATEFUL PACKET FILTERING

- Track status of every TCP connection
  - Track SYN and FIN messages, incoming and outgoing
  - Block packets that don't "make sense"
  - Track timeouts
- Track status of some UDP connections (e.g., DNS)
  - Response should only come if a request comes from inside
- ACL augmented to indicate need to check connection state table

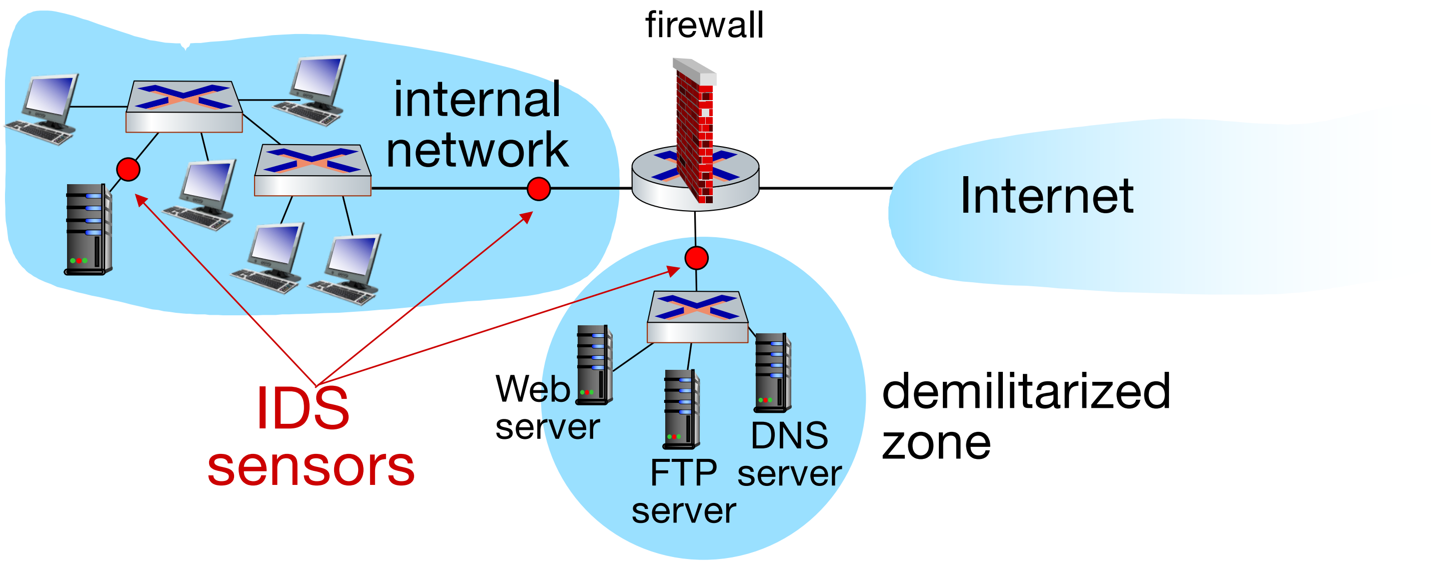
APPLICATION GATEWAYS

- Filter packets based on application data
- Examples:
  - Restriction based on users rather than IP addresses
    - If you provide the wrong password too many times when using your CWL you might be blocked from CS or UBC services
  - Restriction based on DNS hosts or URL patterns
- Can be implemented with a proxy-like structure

INTRUSION DETECTION SYSTEMS

- Packet filtering can operate on headers only
  - No correlation check among sessions
- IDS: Intrusion Detection System
  - Deep packet inspection: look at packet contents
  - Check packets against known attack strings (“signature-based”)
  - Identify statistically unusual traffic (“anomaly-based”)
  - Examine correlation among packets
  - Identify port scanning, network mapping, DoS attacks

INTRUSION DETECTION SYSTEMS



IN-CLASS ACTIVITY

- ICA85