CISSE The Colloquium for Information Systems Security Education

THE COLLOQUIUM 2012
LAKE BUENA VISTA, FL
Monday, June 11 - Wednesday, June 13, 2012

Teaching Stateless and Stateful Firewall Packet Filtering: A Hands-on Approach

Zouheir Trabelsi
UAEU- Faculty of Information Technology

Information Security Program at UAEU

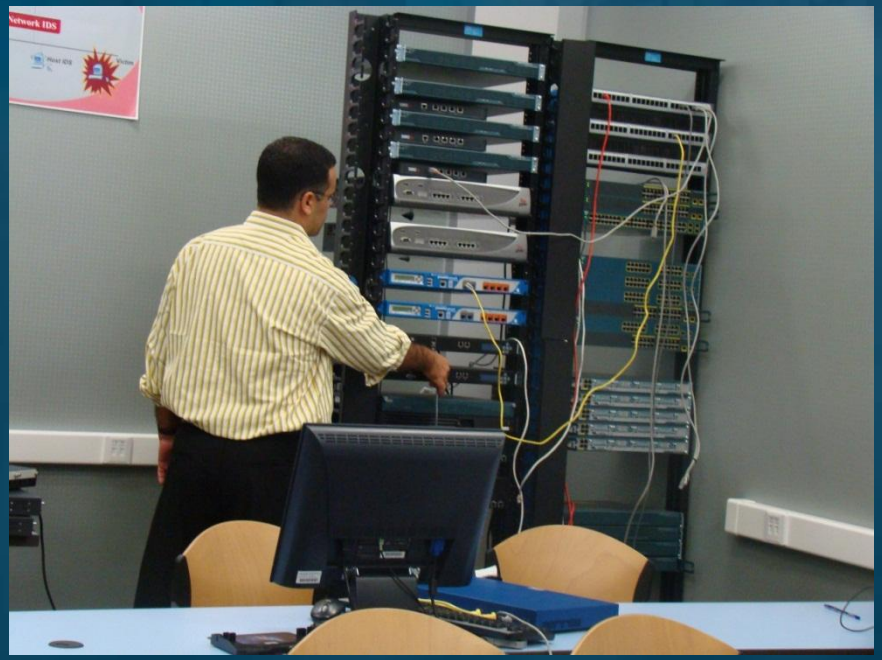
- Cryptography
- Firewall & VPN
- Intrusion Detection and Prevention (IDS/IPS)
- Database security
- OS security
- Biometrics
- Virus & Malicious Code
- Web application security
- Network Traffic Analysis
- Ethical Hacking
- Secure e-transactions
- Wireless Security
- Security Auditing, Penetration testing

State-of-the-Art Security Labs

1 million US$

Intrusion Detection & Prevention Lab

Firewall & VPN Lab

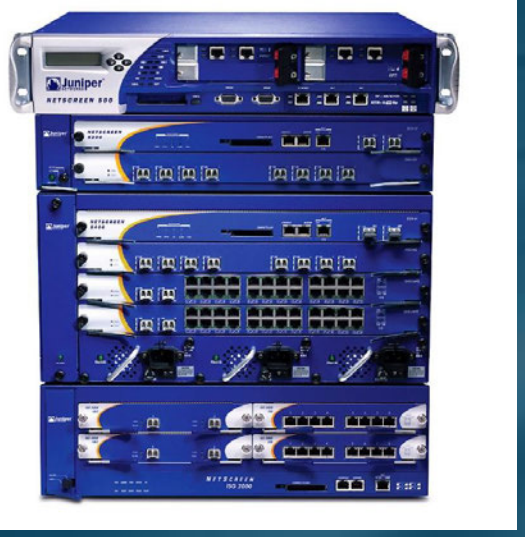


Wireless Security Lab

Cryptography Lab

Biometrics

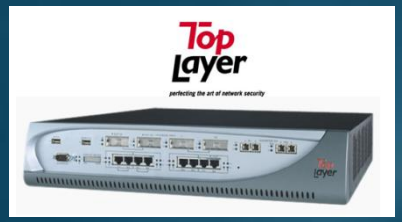
Firewall & VPN Lab

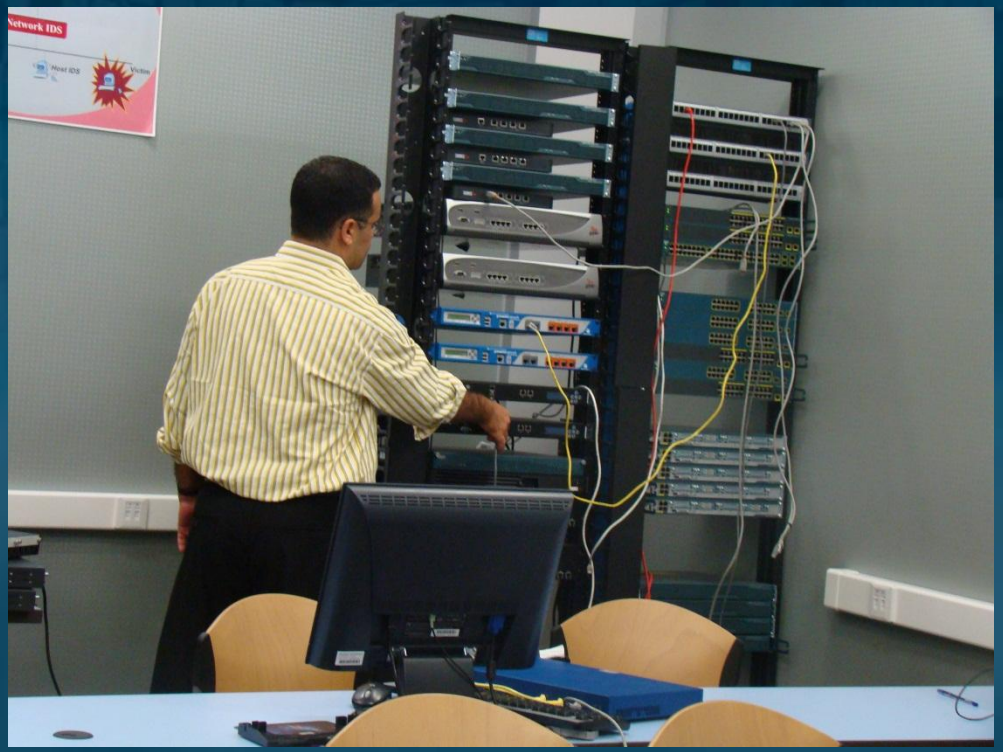


- Basic packet filtering
- Application traffic filtering
- Deep inspection,…

Intrusion Detection & Prevention Lab

Top IDS/IPS devices





- Generate attacks: DoS, MiM,…
- Detect and prevent attacks
- Create attack signatures,…

Biometrics Lab

Iris Recognition

Fingerprint Recognition

Face & Voice Recognition

Handwriting Recognition System

Security Tools (Open source & Commercial)

Penetration testing

Penetration testing

LanGuard: Network Security Auditing

- CommView sniffer for wired LANs
- CommView for WiFi sniffer for WLAN
- AirCrack
- Can & Abel, …

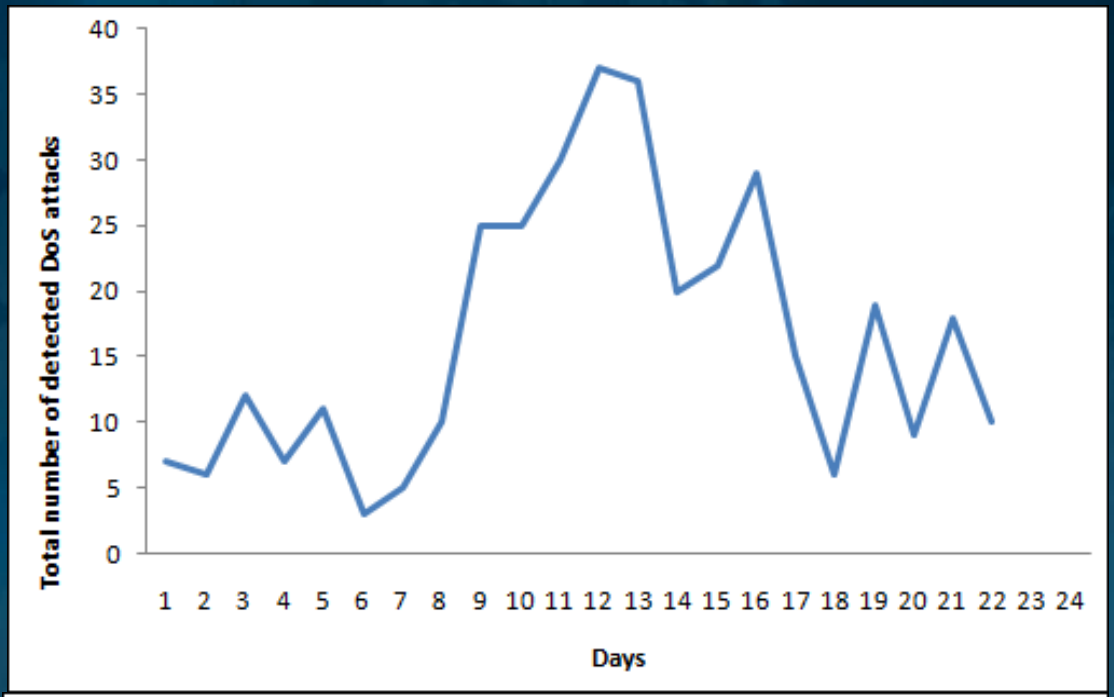
Information Security Program (Undergraduate)

Hands-on Lab Exercises

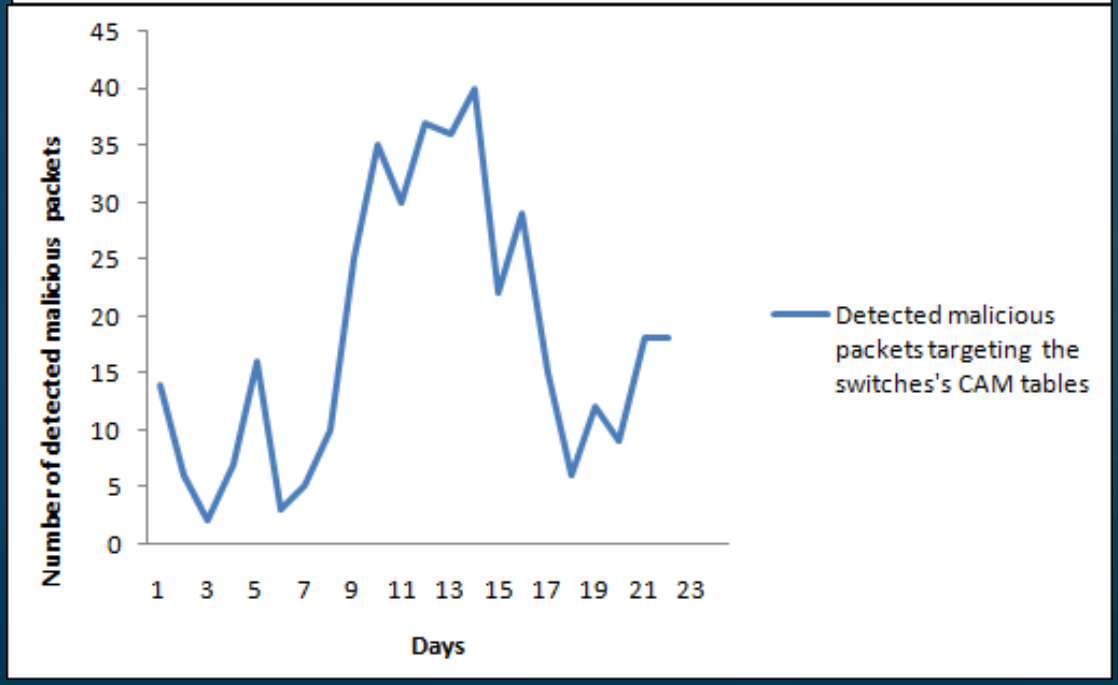
Defense techniques

Offensive techniques (Ethical hacking)

- Better anatomize the concepts
- Hands-on skills



Evolution of the number of DoS attacks detected by the university's IDS sensors



Evolution of the number of detected malicious IP and ARP packets targeting the switches' CAM tables

Paper:

Teaching Stateless and Stateful Firewall Packet Filtering: A Hands-on Approach

Information Security Program

Basic packet filtering

Stateless & Stateful firewall concept

Firewall technologies

Packet classification

Filtering mechanisms

…

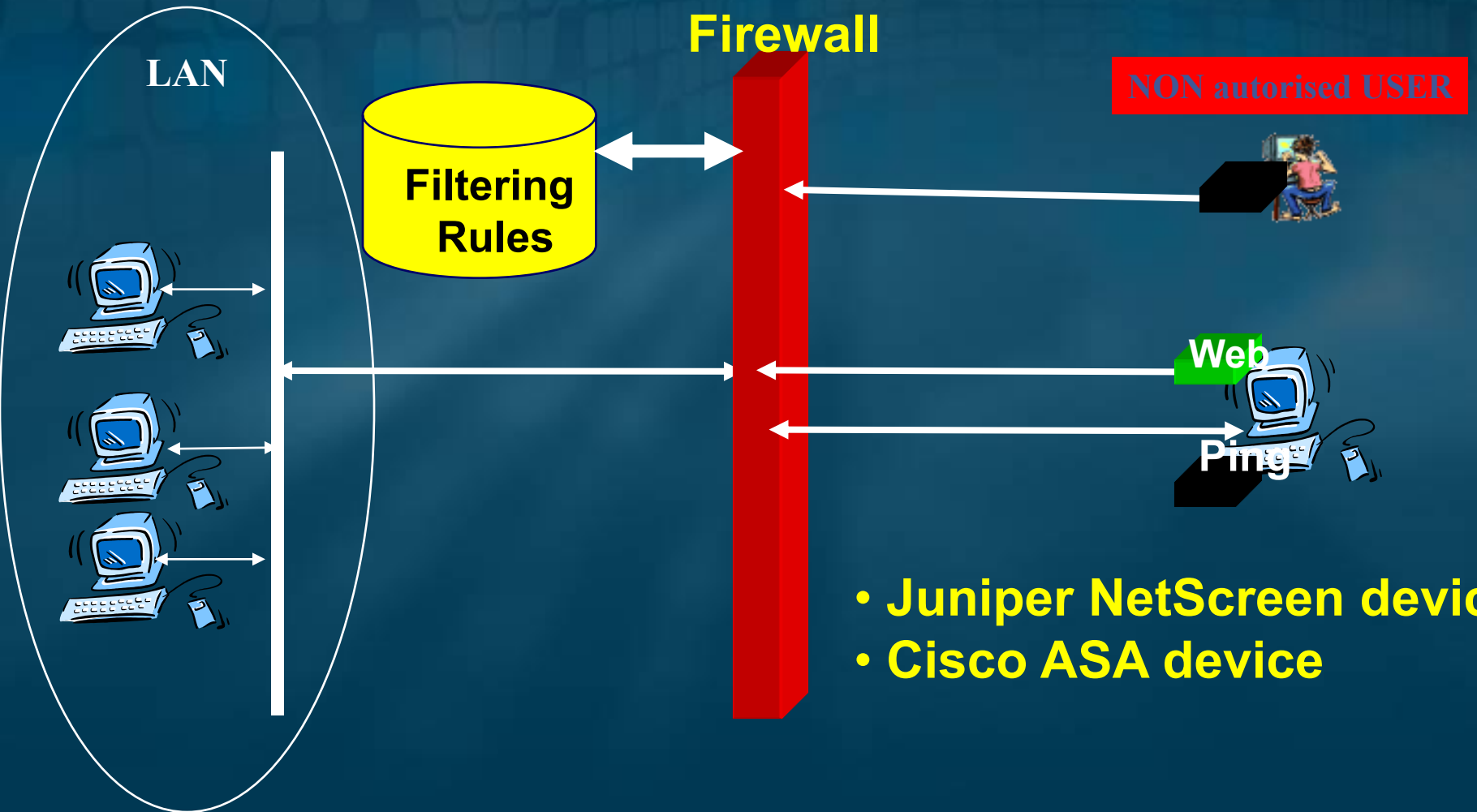
Paper

Hands-on lab exercise:

How to identify whether a given firewall performs stateless or stateful packet filtering.

The learning objective: *better anatomize the concept of stateless and stateful firewall packet filtering through examples and experiments in an isolated network laboratory.*

Incoming /outgoing Network Traffic Filtering

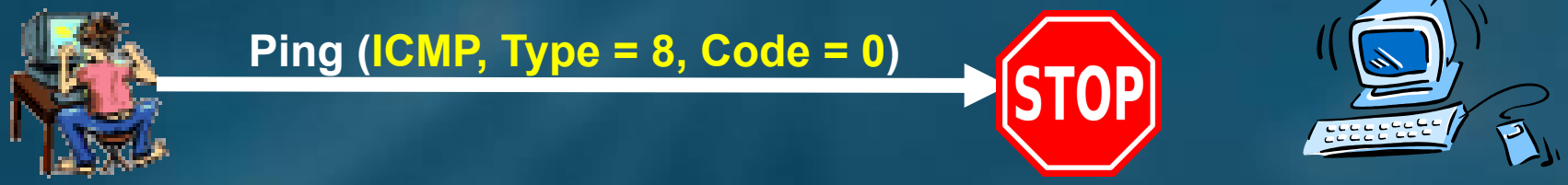


- Juniper NetScreen device
- Cisco ASA device

Security Policy → Filtering Rules

Example of security policy:

- I want to DENY all incoming Ping request



Filtering rule:

Rule	Direction	Source IP	Destination IP	Protocol	Type	Code	Action
R1	Incoming	Any	My IP	ICMP	8	0	Deny

Stateless and Stateful Firewall Concepts

Concept: Stateless & Stateful Firewalls

Stateful firewall: is able to memorize and identify the status of:

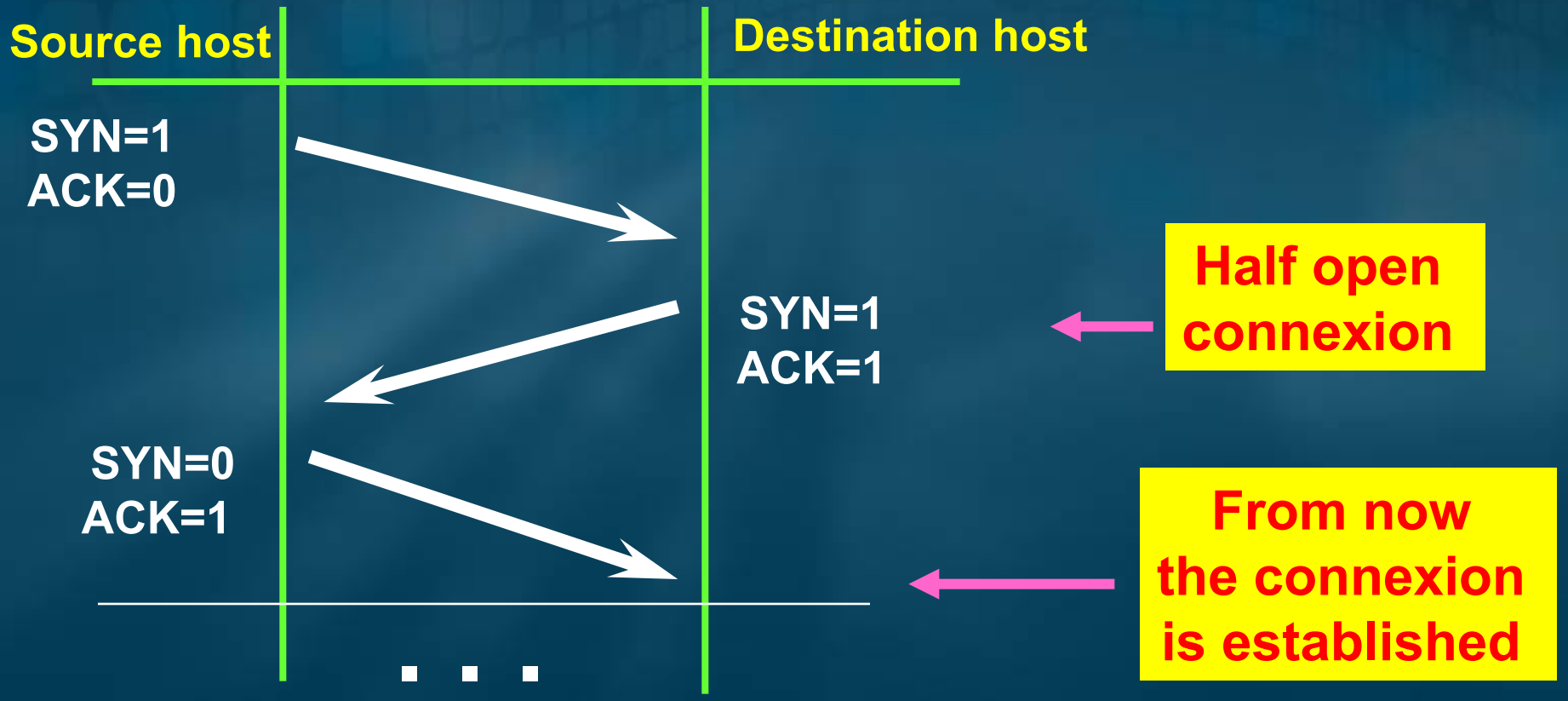
- **TCP sessions**
- **UDP sessions**
- **ICMP request/reply traffic**

A stateless firewall has:

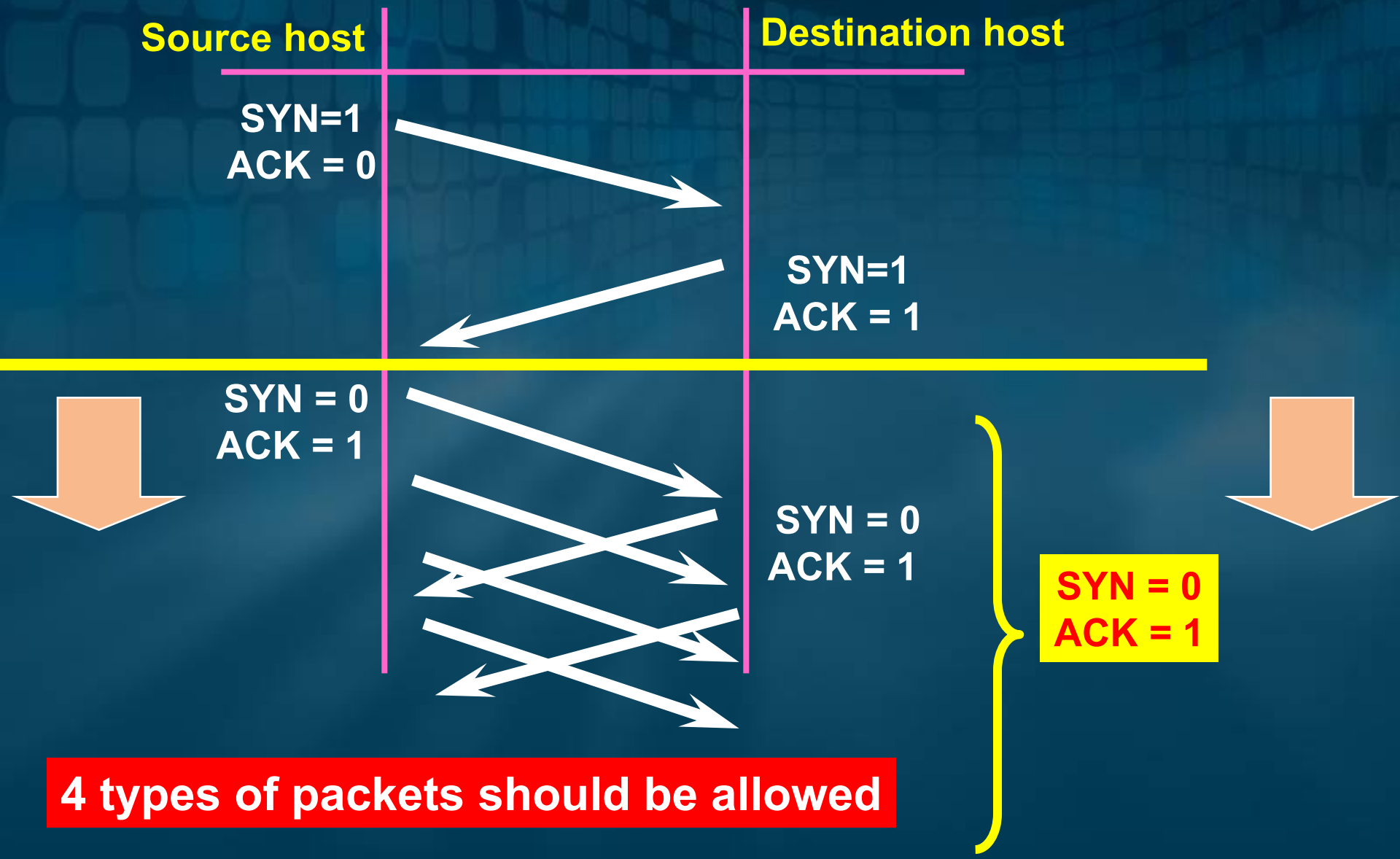
No mechanism to identify packets that belong to established sessions

Opening a TCP session:
Three-way handshake

TCP Connexion establishment :

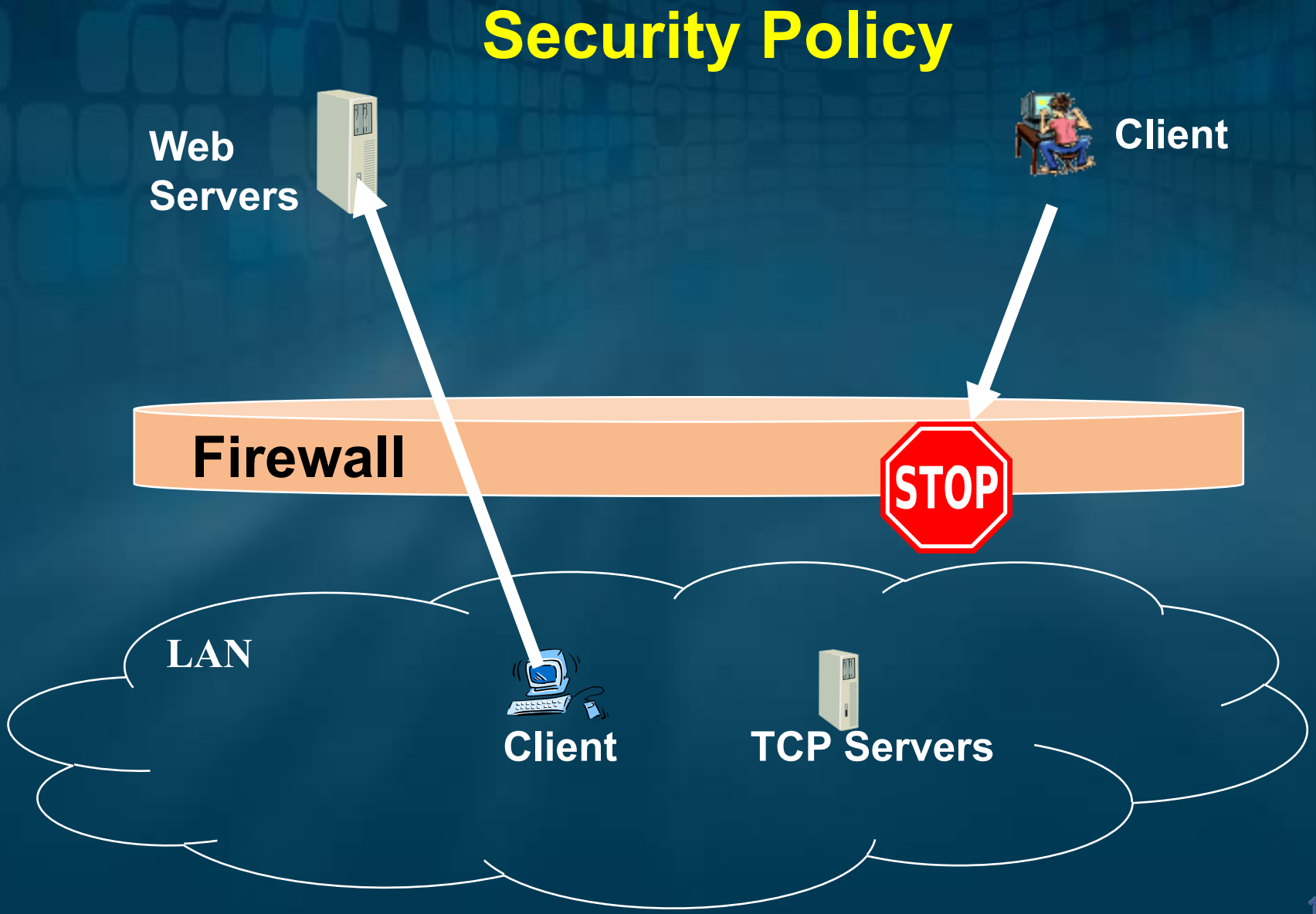


SYN & ACK bits in the TCP Header



4 types of packets should be allowed

Stateless and Stateful Firewall Concept (TCP sessions)



Stateless and Stateful Firewall

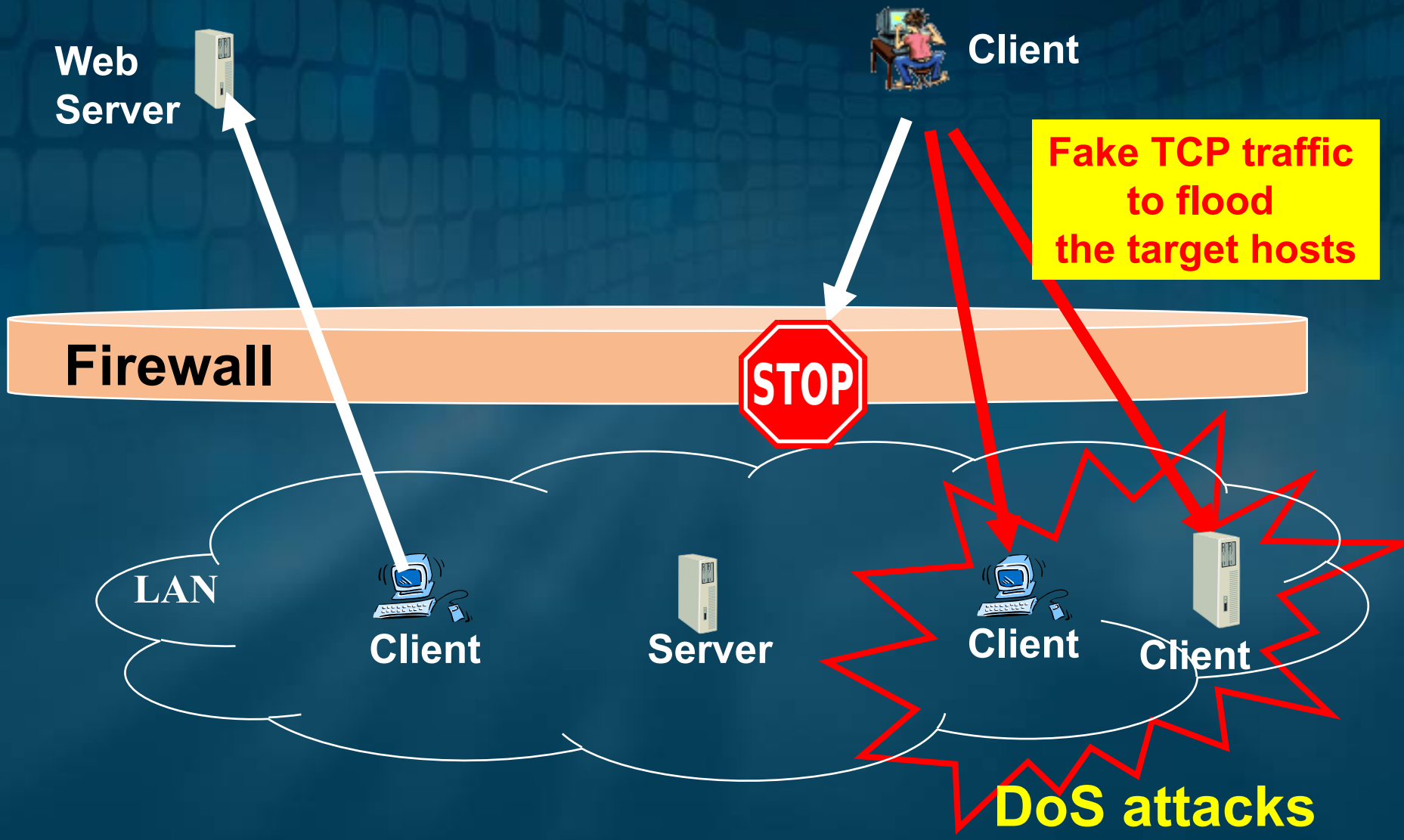
Security policy:

- Our hosts are ALLOWED to access any external web server (TCP/80)
- External hosts are NOT ALLOWED to access any TCP service in our LAN

Filtering rules :

Direction	Source IP	Dest. IP	Protocole	Sour. Port	Dest. Port	SYN bit	ACK bit	Action
Out	LAN	Externe	TCP	Any	80	1	0	Accept
In	Externe	LAN	TCP	80	Any	1	1	Accept
Out	LAN	Externe	TCP	Any	80	0	1	Accept
In	Externe	LAN	TCP	80	Any	0	1	Accept
In	Externe	LAN	TCP	Any	Any	1	0	Deny

Stateless and Stateful Firewall



Stateless and Stateful Firewall

Filtering rules :

Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK	Action
Out	LAN	Externe	TCP	Any	80	1	0	Accept
In	Externe	LAN	TCP	80	Any	1	1	Accept
Out	LAN	Externe	TCP	Any	80	0	1	Accept
In	Externe	LAN	TCP	80	Any	0	1	Accept
In	Externe	LAN	TCP	Any	Any	1	0	Deny

Packet:

Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK
In	Externe	LAN	TCP	Any	80	1	0

External hosts cannot establish a connection with our hosts

This packet will be rejected

Stateless and Stateful Firewall

Filtering rules :

Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK	Action
Out	LAN	Externe	TCP	Any	80	1	0	Accept
In	Externe	LAN	TCP	80	Any	1	1	Accept
Out	LAN	Externe	TCP	Any	80	0	1	Accept
In	Externe	LAN	TCP	80	Any	0	1	Accept
In	Externe	LAN	TCP	Any	Any	1	0	Deny

Packet:

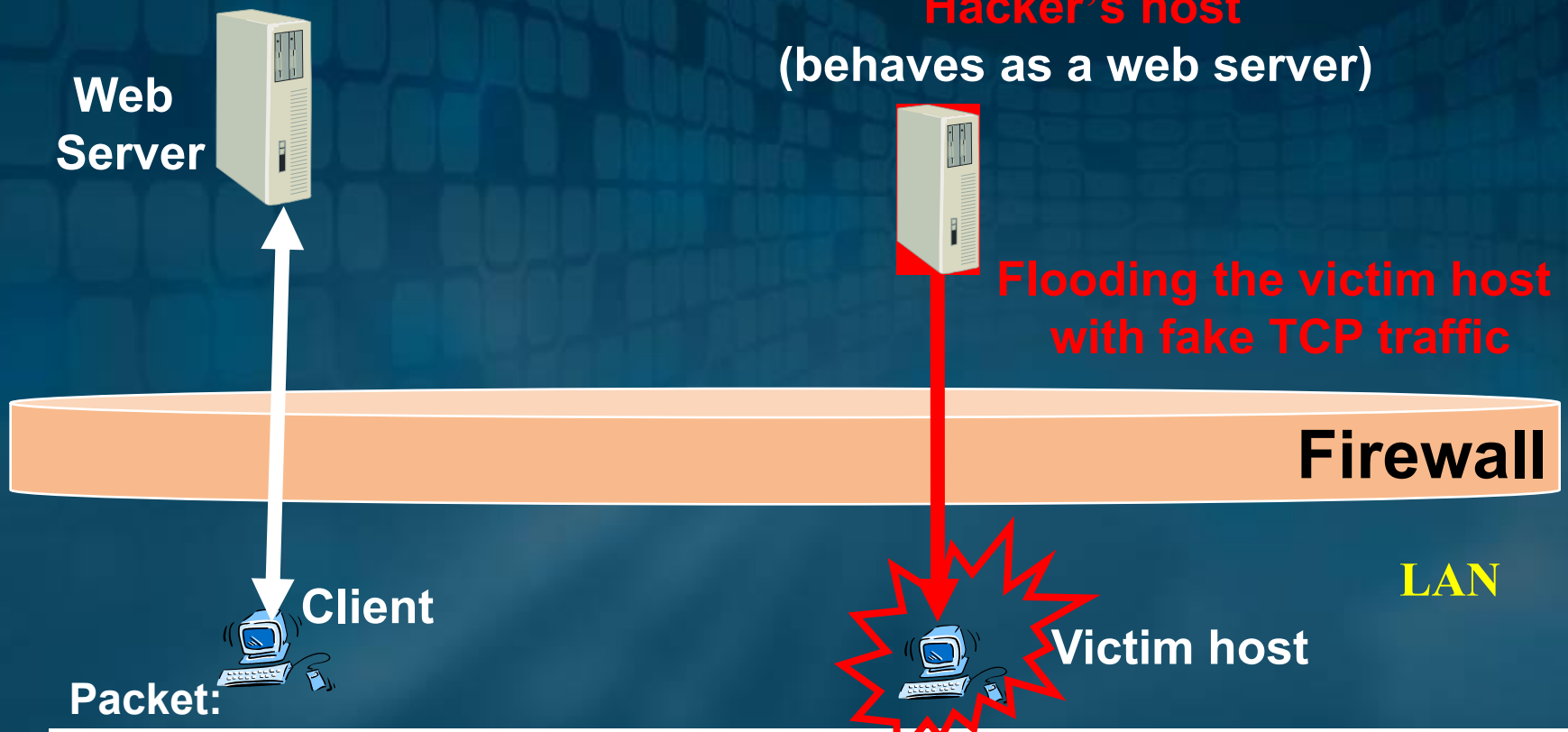
Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK
In	Externe	LAN	TCP	7000	80	1	0
In	Externe	LAN	TCP	80	9000	0	1

Our hosts are NOT protected from this malicious packet.

This packet will be accepted

This packet will be rejected

Stateless and Stateful Firewall



Packet:

Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK
In	Externe	LAN	TCP	7000	80	1	0
In	Externe	LAN	TCP	80	9000	0	1

This packet will be accepted

This packet will be rejected

Stateful Firewall

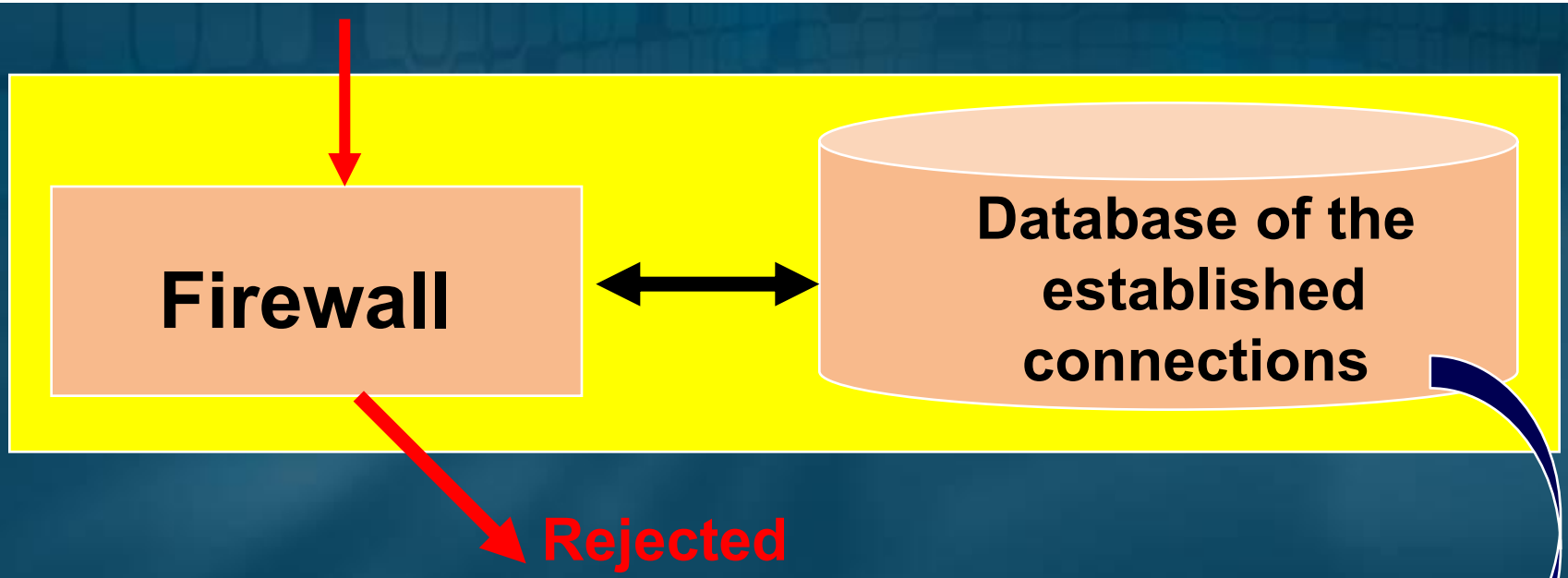
Database of the established connections

Source IP	Dest. IP	Protocole	Source Port	Destination Port	status
Client#1	Web server#1	TCP	4000 (for example)	80	established
Client #2	Web server #2	TCP	5000 (for example)	80	established

Stateful Firewall

Incoming TCP Packet:

Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK
In	Externe	LAN	TCP	80	3000	0	1



Database of established connections:

Source IP	Dest. IP	Protocole	Source Port	Destination Port	status
Client	Web server	TCP	4000	80	Full established

Stateless and Stateful Firewalls

Malicious packet

Direction	Source IP	Dest. IP	Proto	Sour. Port	Dest. Port	SYN	ACK
In	Externe	LAN	TCP	80	Any	0	1

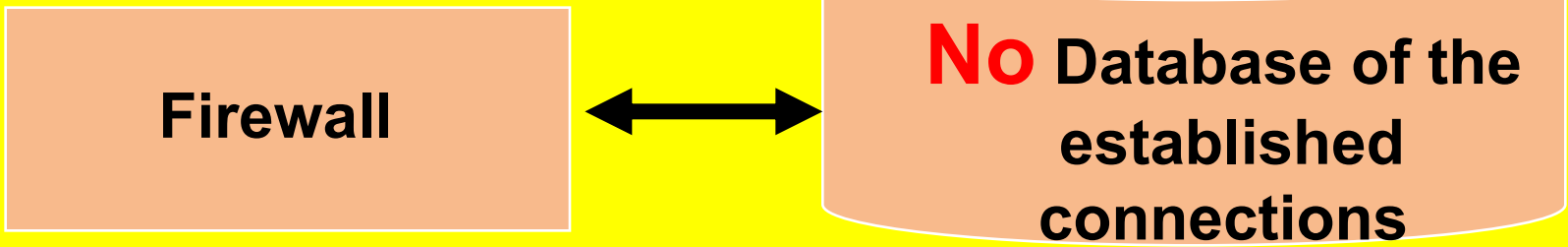
Stateless Firewall → *Accepted*

Stateful Firewall → *Rejected*

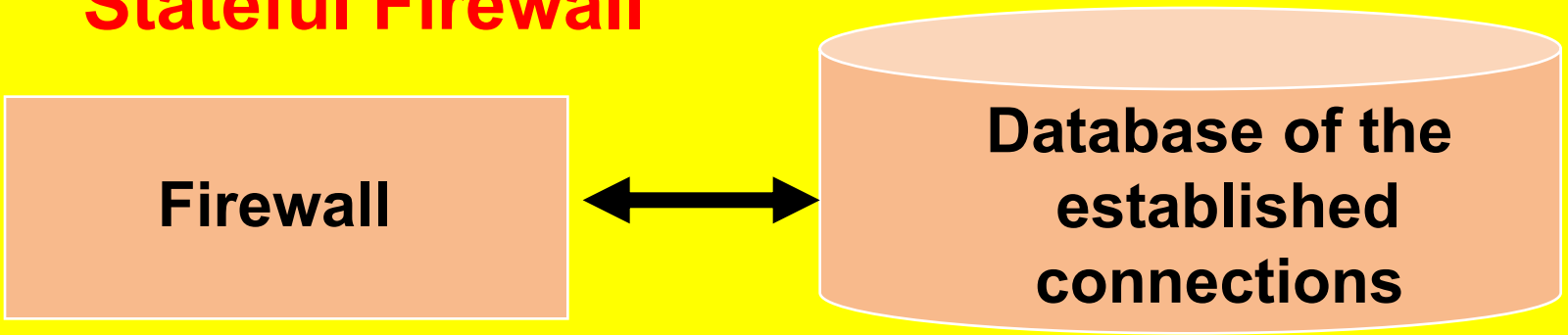
LAN's hosts are protected from malicious packets used to generate DoS attacks

Stateless and Stateful Firewall

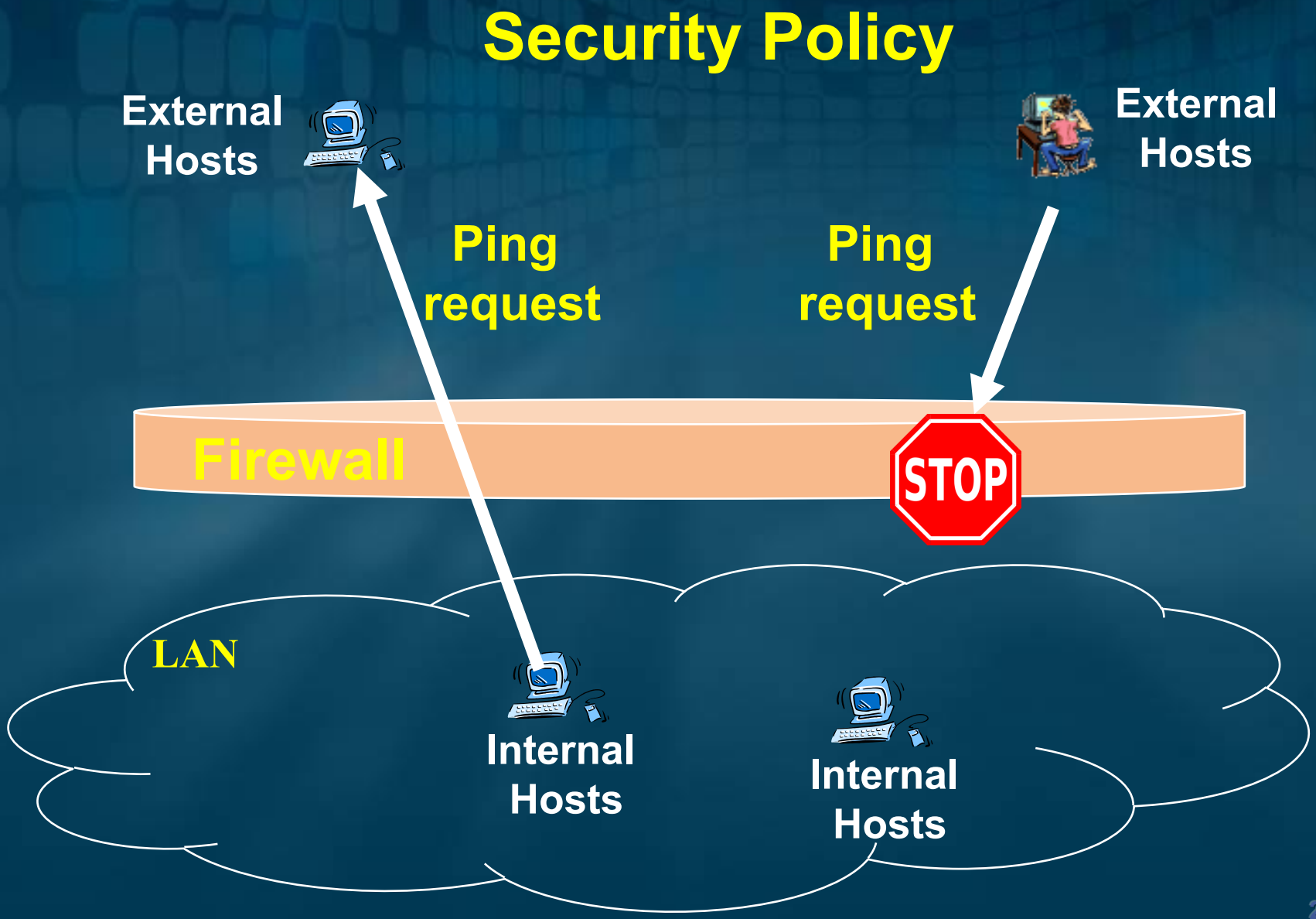
Stateless Firewall



Stateful Firewall



Stateless and Stateful Firewall Concept (ICMP traffic: Ping)



Example of security policy:

- Deny incoming Ping
- Allow outgoing Ping

Ping (ICMP, Type = 8, Code = 0)

My host

Ping (ICMP, Type = 8, Code = 0)

Ping (ICMP, Type = 0, Code = 0)

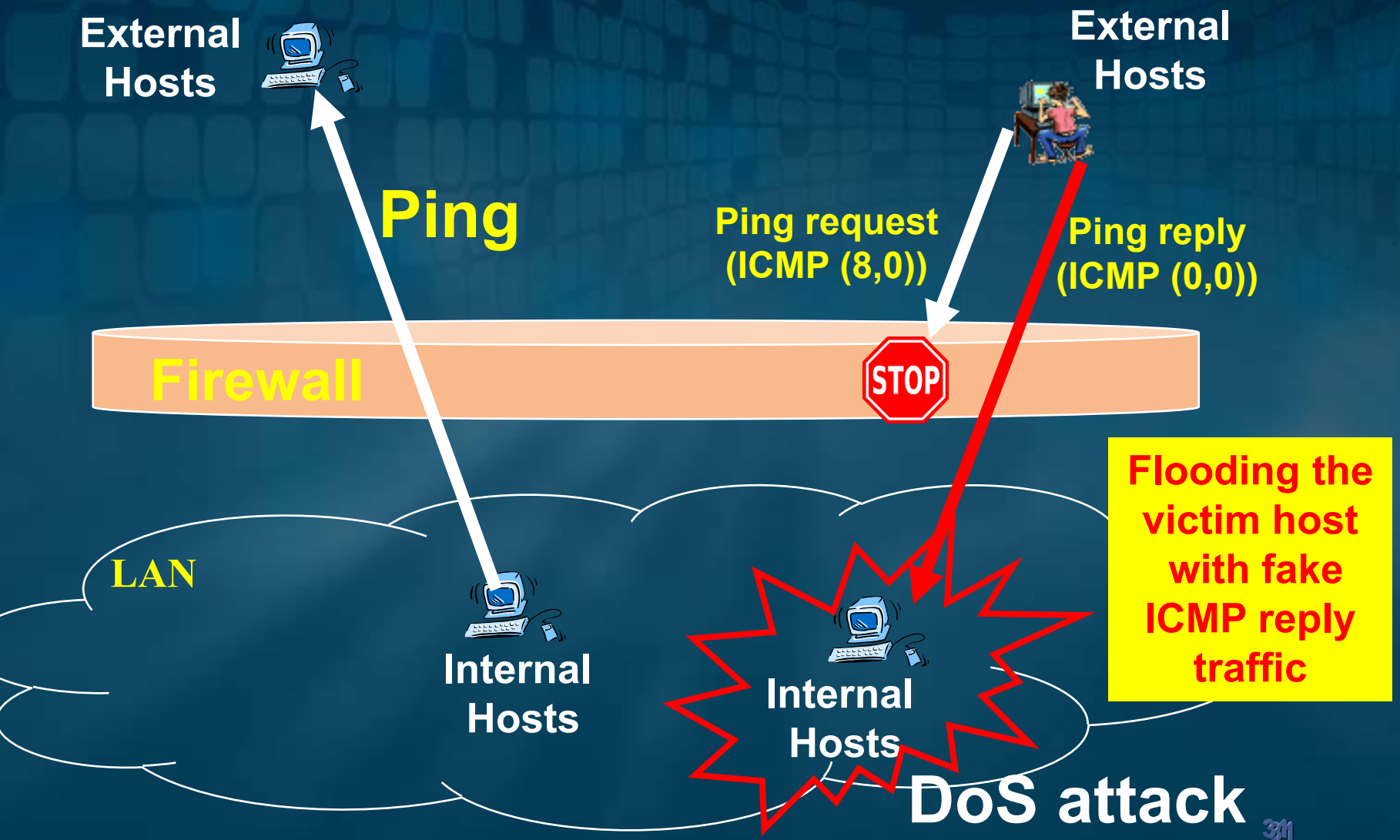
Rule	Direction	Source IP	Destination IP	Protocol	Type	Code	Action
R1	Incoming	Any	My IP	ICMP	8	0	Deny

Rule	Direction	Source IP	Destination IP	Protocol	Type	Code	Action
R2	Outgoing	My IP	Any	ICMP	8	0	Allow

Rule	Direction	Source IP	Destination IP	Protocol	Type	Code	Action
R3	Incoming	Any	My IP	ICMP	0	0	Allow

30

Stateless Firewall for ICMP traffic



To better anatomize the concepts of stateless and stateful firewall

Hands-on lab exercise:

describes steps to identify whether the Cisco ASA 5520 Firewall offers stateful or stateless TCP and ICMP packet filtering.

The experiment's steps can be used to test any other firewall device or software

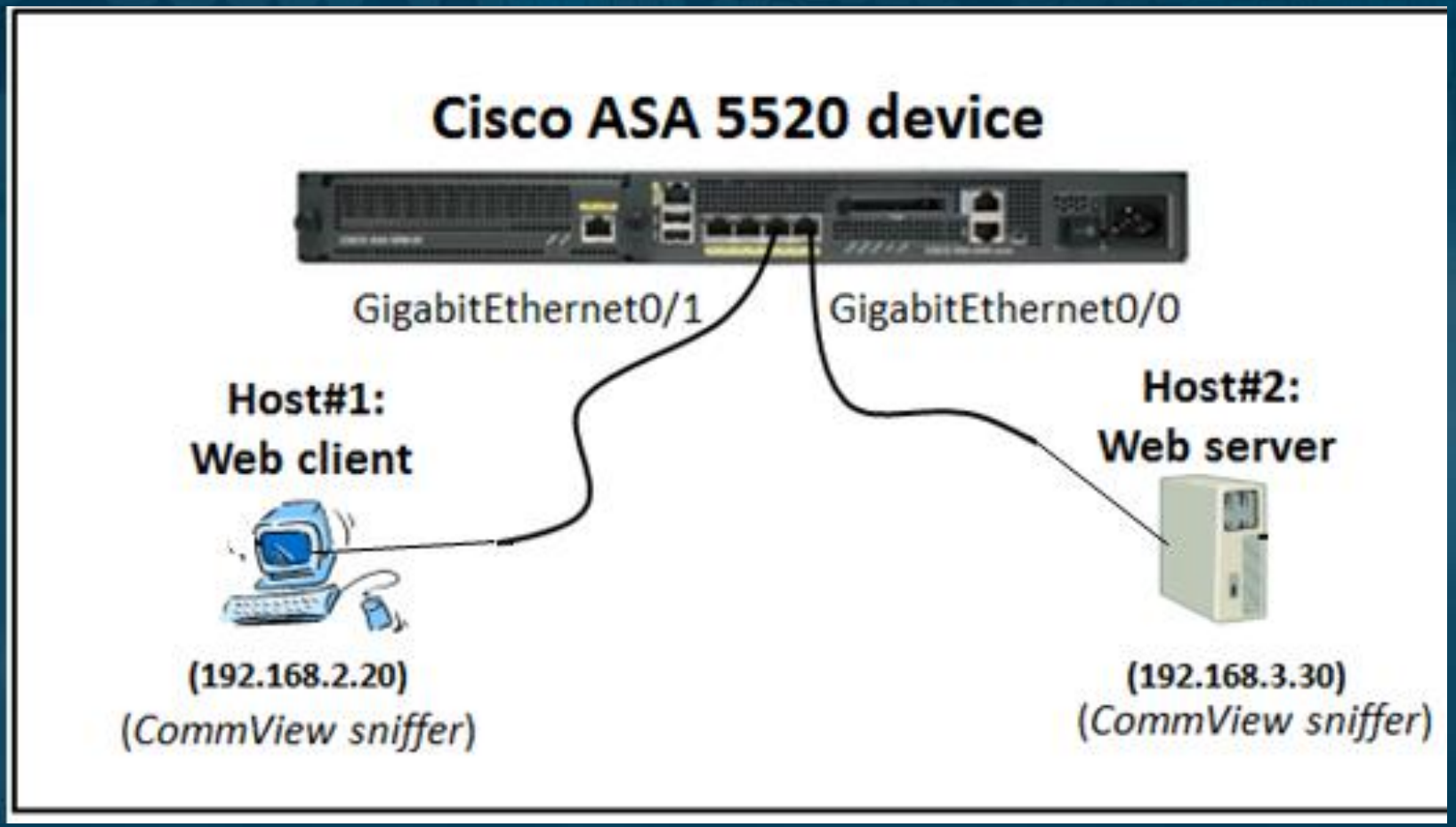
Cisco ASA 5520 :
Stateless or Stateful Firewall?

The two experiments:

Exp. 1: Stateful **TCP** packet filtering testing

Exp. 2: Stateful **ICMP** packet filtering testing

Network Architecture



Exp. 1:
Stateful TCP packet filtering testing

Exp. 1: Stateful TCP packet filtering testing

Step 1: Host #1 accesses the Web site in host #2

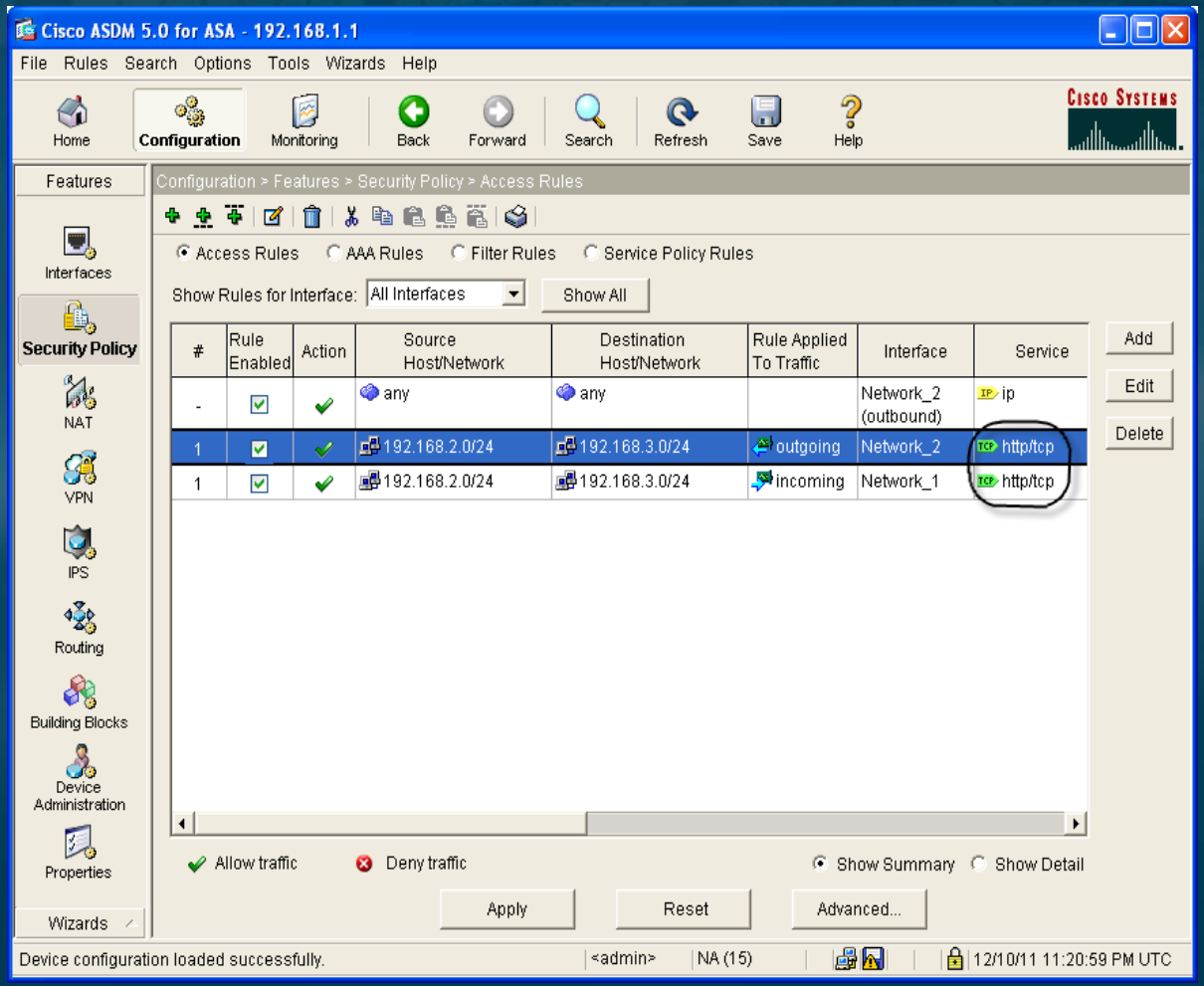
Step 2: Sniff the Web session traffic

Step 3: Host #1 generates a FAKE TCP packet

Step 4: Analyze the results and identify the type of firewall

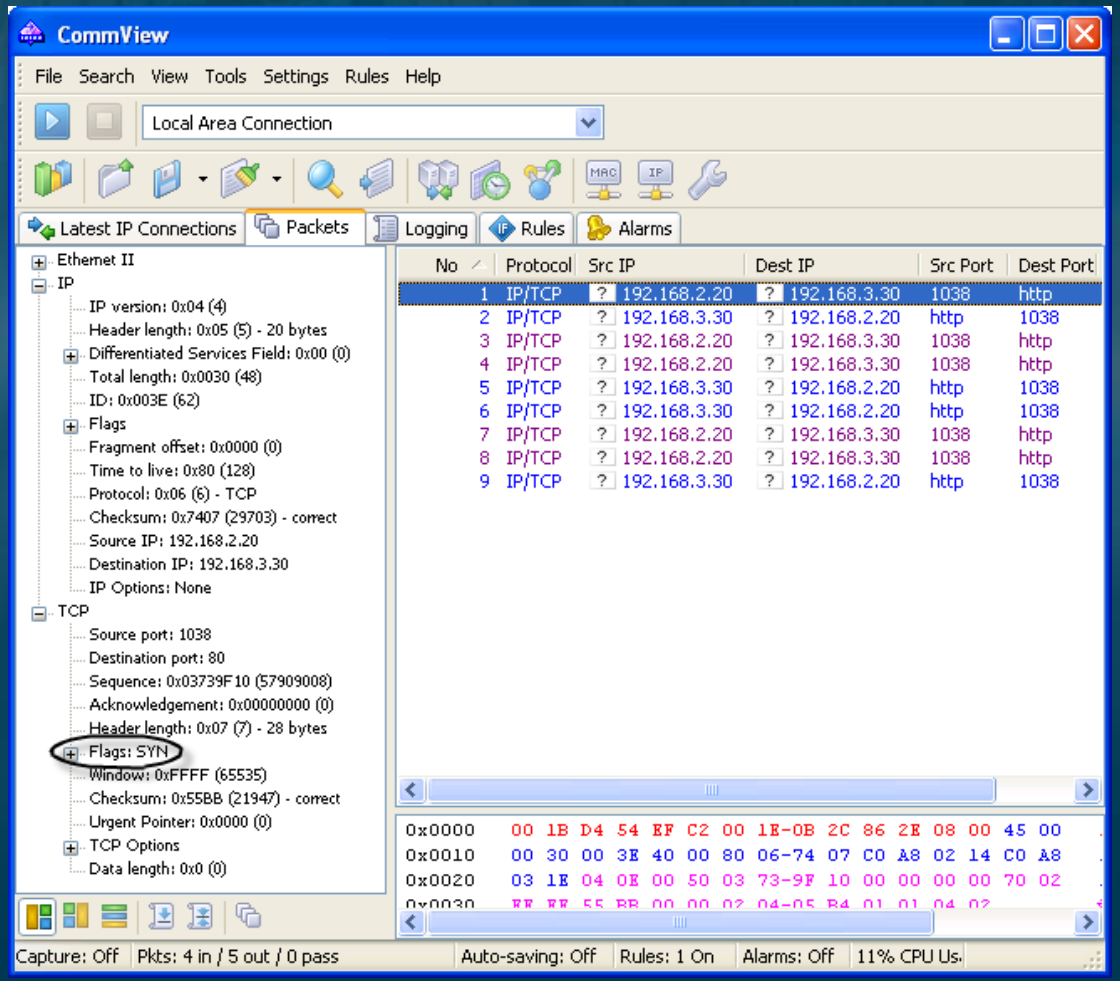
Exp. #1:

Security policy: Allow web traffic (TCP/80) between the Web client (Host#1) and the Web server (Host#2).



From Host#1, a Web browser is used to connect to the Web server at Host#2

At Host#1, CommView sniffer is used to capture the three-way handshake TCP packets of the Web session.

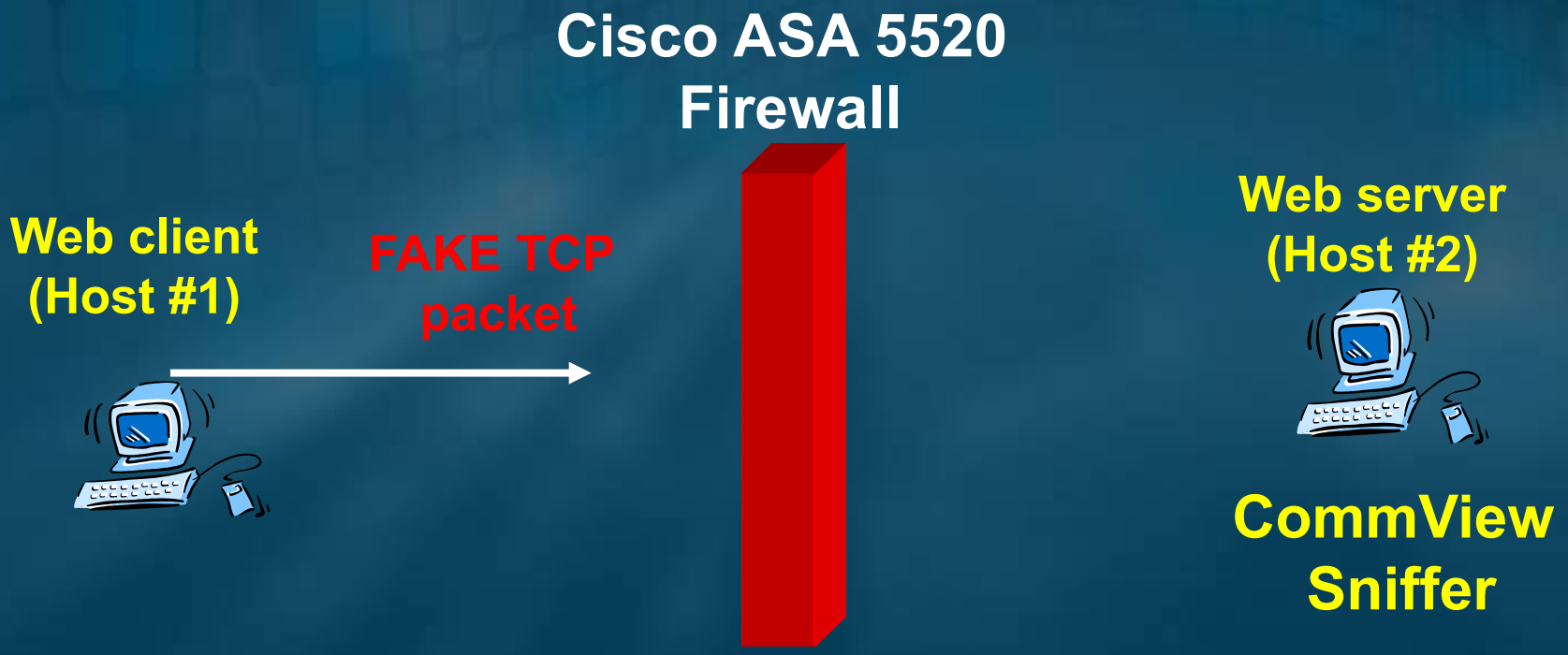


Collect the values of the main fields of the captured three-way handshake packets (characterizing the Web session):

Example:

Packet number as displayed in CommView sniffer	Source IP	Destination IP	Source port	Destination port	SYN	ACK
1	192.168.2.20	192.168.3.30	1038	80	1	0
2	192.168.3.30	192.168.2.20	80	1038	1	1
3	192.168.2.20	192.168.3.30	1038	80	0	1

Using a packet generator, a FAKE TCP packet pretending that a TCP connection on port 80 is already established (SYN = 0 and ACK = 1), is sent to Host #2:



Established TCP session:

Packet number as displayed in CommView sniffer	Source IP	Destination IP	Source port	Destination port	SYN	ACK
1	192.168.2.20	192.168.3.30	1038	80	1	0
2	192.168.3.30	192.168.2.20	80	1038	1	1
3	192.168.2.20	192.168.3.30	1038	80	0	1

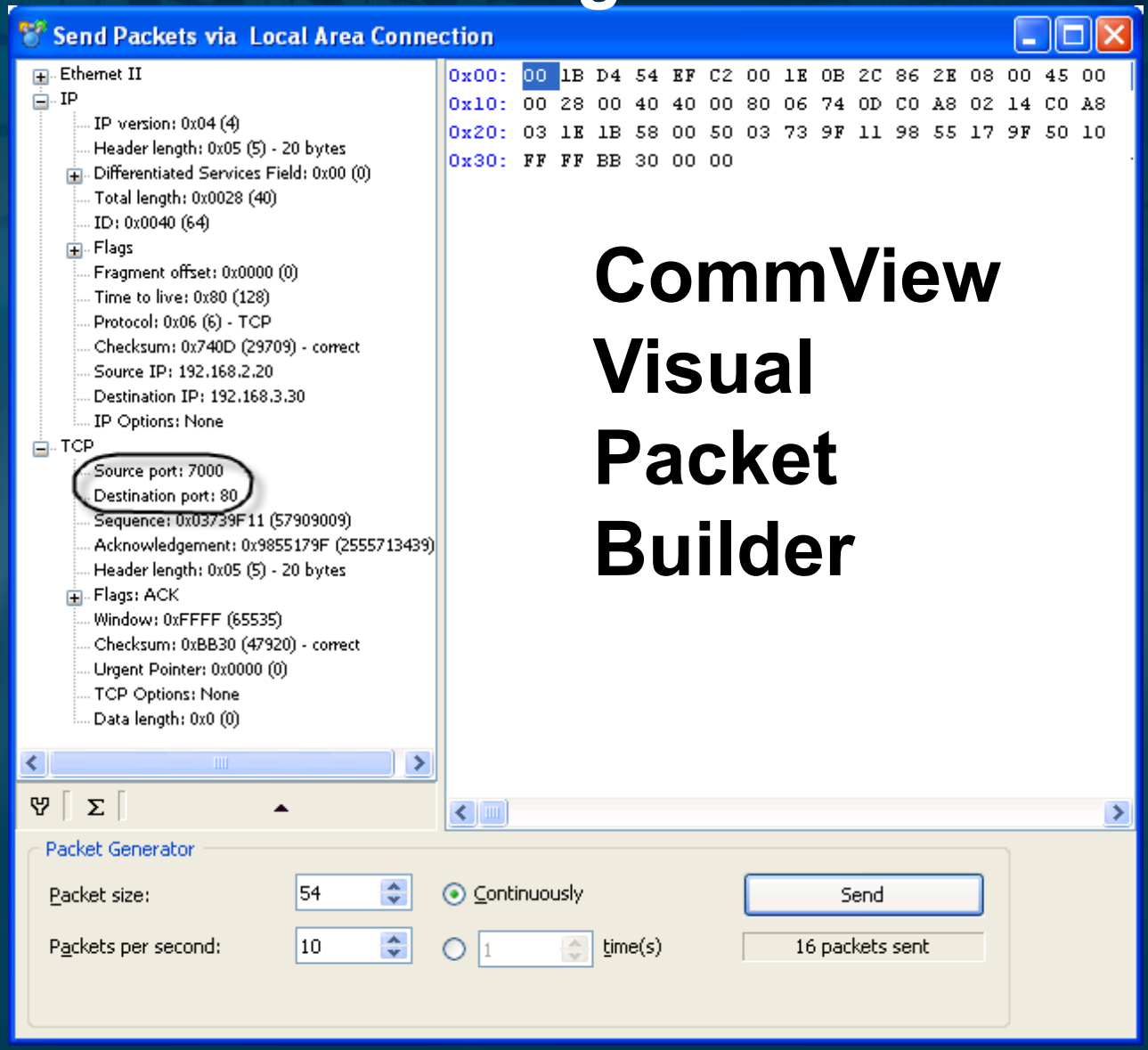
The FAKE TCP packet includes a source port different from the source port of the current active Web session.

FAKE TCP packet:

Source IP	Destination IP	Source port	Destination port	SYN	ACK
192.168.2.20	192.168.3.30	7000	80	0	1

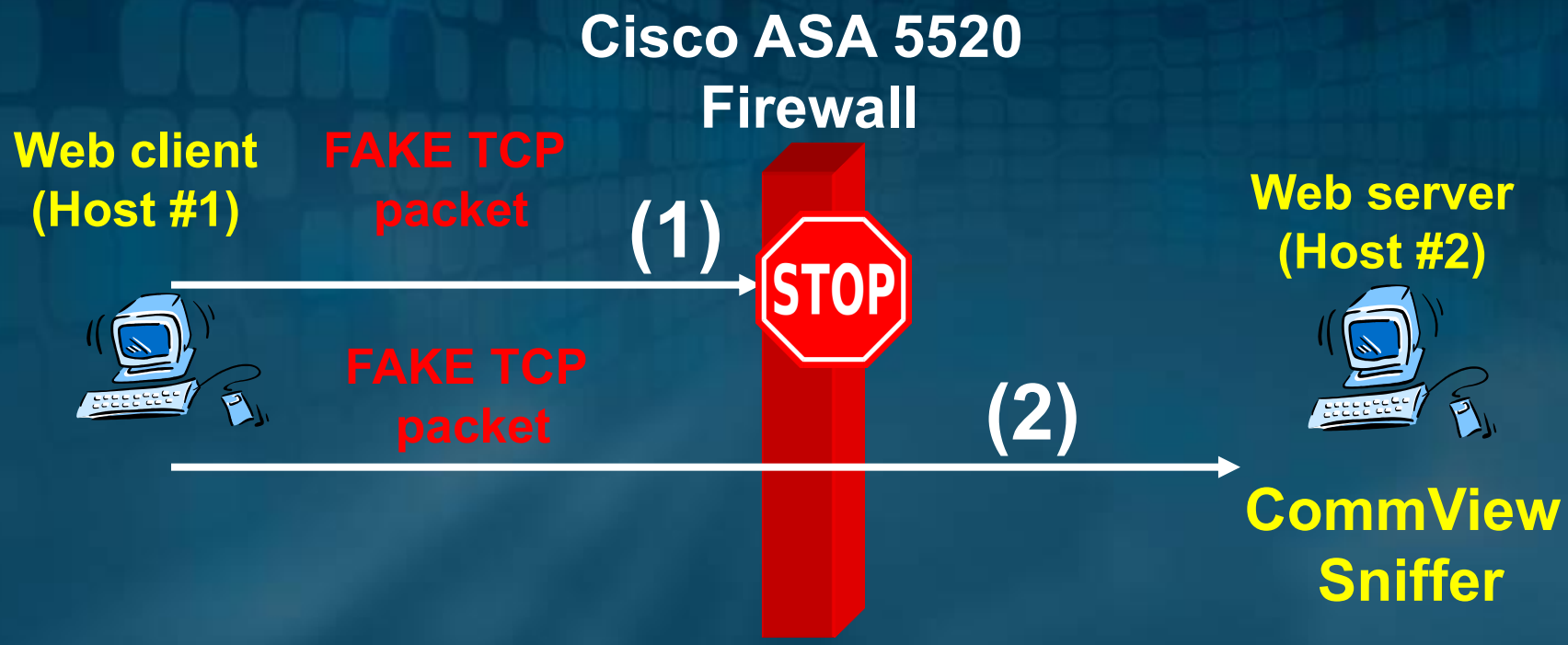
FAKE TCP packet:

Packet generator tool:



CommView Visual Packet Builder

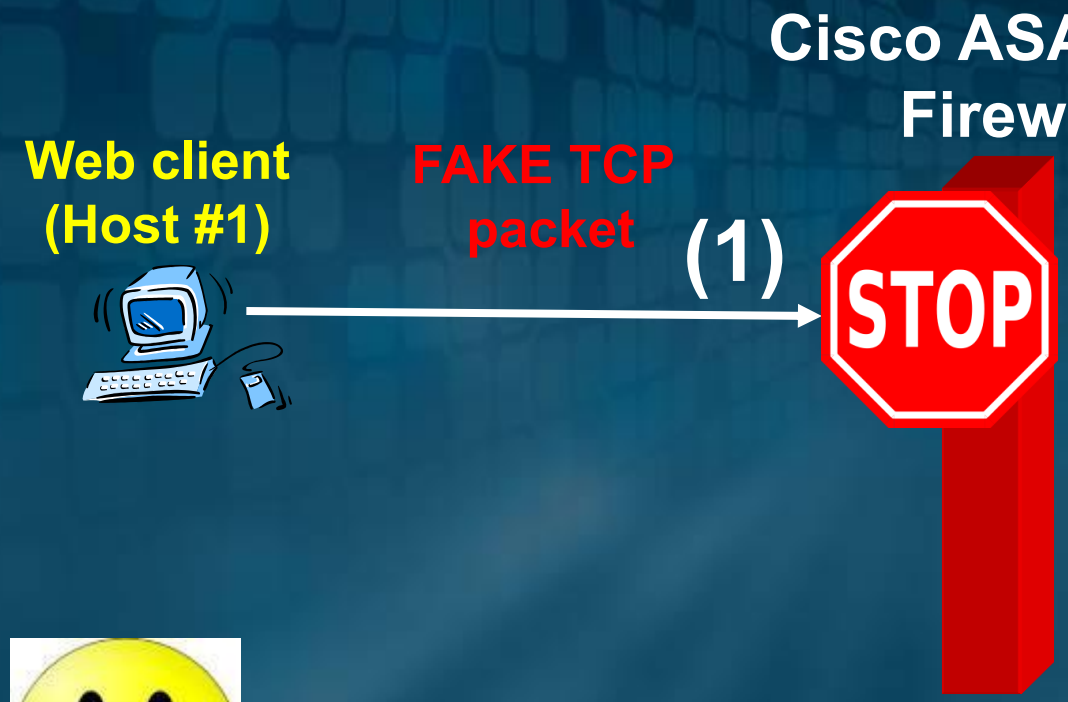
Two possible cases:



(1): Cisco ASA offers **stateful** TCP packet filtering

(2): Cisco ASA offers **stateless** TCP packet filtering

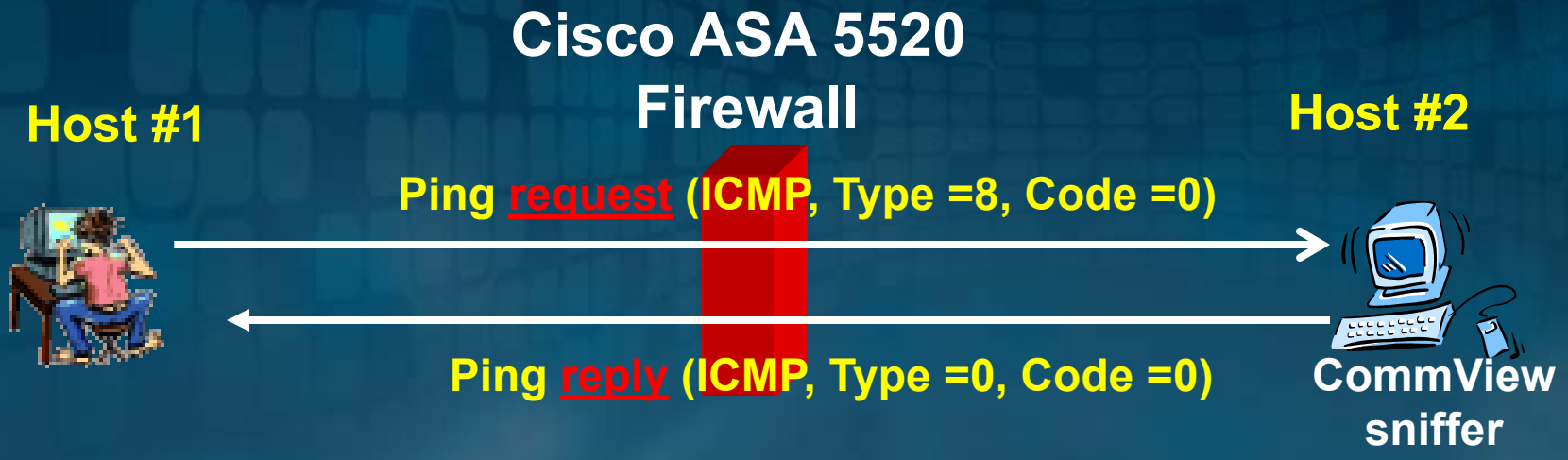
Experiment Result



Cisco ASA 5520 is a stateful firewall for TCP related traffic, since it denies TCP packets that do not belong to established TCP sessions

Exp. 2:
Stateful ICMP packet filtering testing

Exp. 2: Stateful ICMP packet filtering testing



Step 1: Host #1 pings host #2

Step 2: Sniff the Ping traffic

Step 3: Host #2 generates a FAKE ICMP reply packet

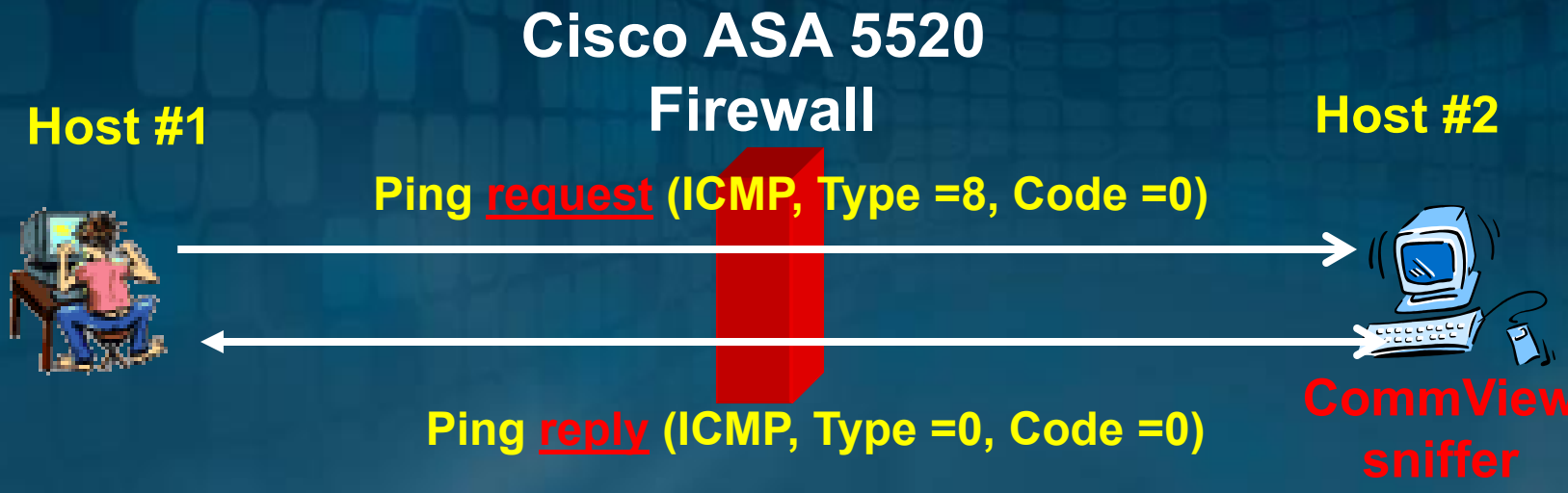
Step 4: Analyze the results and identify the type of firewall

Exp. 2: Stateful ICMP packet filtering testing

Security policy:

Allow Host #1 to ping Host #2, but Host #2 is not allowed to ping Host #1.

Exp. 2: Stateful ICMP packet filtering testing



Host #1 pings Host #2

At Host #1, CommView sniffer is used to capture the exchanged ICMP packets.

The values of the main fields of the exchanged ICMP request and reply packets

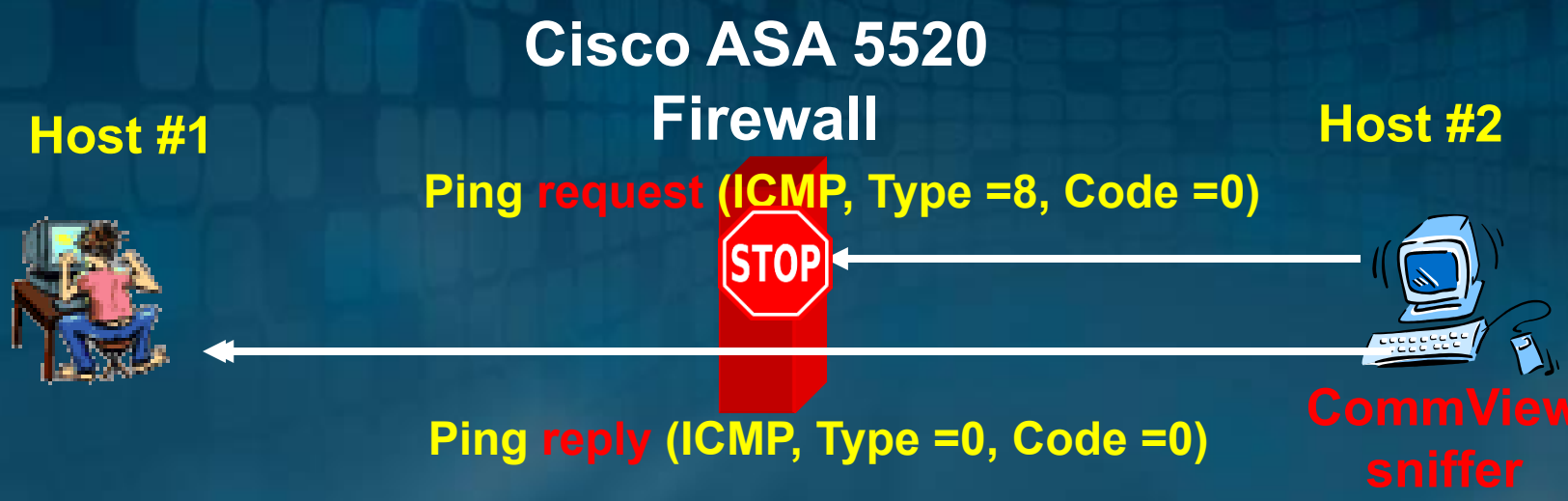
Packet number as displayed in CommView	Source IP	Destination IP	Type	Code	Identifier	Sequence Number
1	192.168.2.20	192.168.3.30	8	0	512	9472
2	192.168.3.30	192.168.2.20	0	0	512	9472

Then, CommView Visual Packet Builder is used to send from Host #2 to Host #1 a fake ICMP echo reply packet, pretending that an ICMP echo request packet has been received before from Host#1.

Example of Fake ICMP echo reply packet:

Source IP	Destination IP	Type	Code	Identifier	Sequence Number
192.168.3.30	192.168.2.20	0	0	512	8000

Experiment Result:



Consequently, the Cisco ASA 5520 is a stateless firewall for ICMP related traffic, since it did not deny the fake ICMP echo reply packet.

Cisco ASA 5520 Firewall

Stateful TCP packet filtering

Stateless ICMP packet filtering

Hands-on Lab outcomes:

- Better anatomize the concept of stateful and stateless packet filtering
- Test firewalls
- Generate fake packets
- Analyze network traffic using sniffer

STUDENT'S PERFORMANCE AND SATISFACTION

Stateless and Stateful concepts: Network Border Control course (SECB358).

From **fall 2006 to spring 2008**: students enrolled in SECB358 course were not offered hands-on lab exercises on stateless and stateful packet filtering.

Only the conceptual part of the topic has been described in the class.

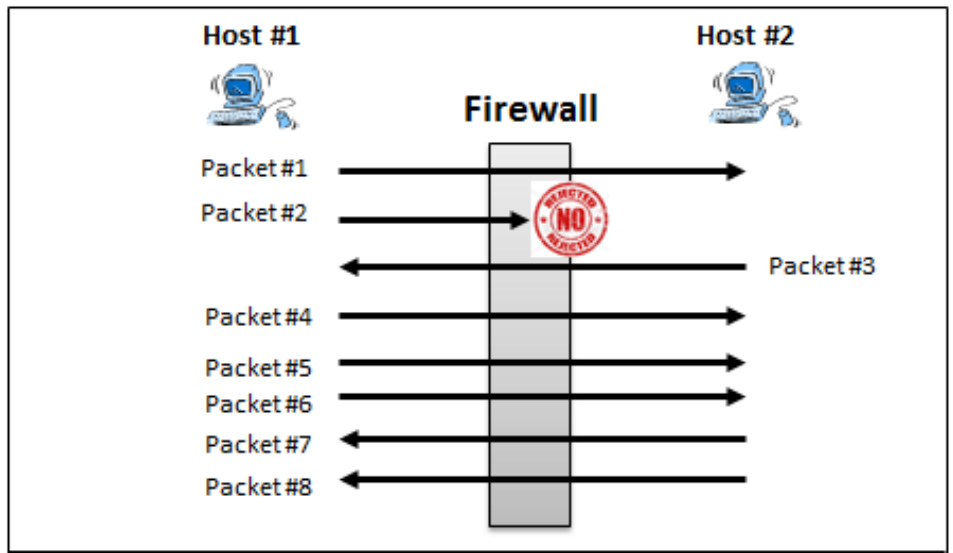
However, from **fall 2008 to spring 2011**, the students were offered the hands-on lab exercise described in this paper.

Over the **five year period**, each semester the students were given two quizzes and a Midterm exam exercise about stateless and stateful packet filtering

QUIZ EXAMPLE

Tell if the firewall performs stateless or stateful packet inspection for TCP traffic,

and (2) tell if the firewall performs stateless or stateful packet inspection for ICMP traffic



TCP packets

Packet #1 : (TCP, S-Port=2000, D-Port=21, SYN=1, ACK=0)

Packet #2 : (TCP, S-Port=2001, D-Port=21, SYN=0, ACK=1)

Packet #3 : (TCP, S-Port=21, D-Port=2000, SYN=1, ACK=1)

Packet #4 : (TCP, S-Port=2000, D-Port=21, SYN=0, ACK=1)

Packet #5 : (TCP, S-Port=2002, D-Port=23, SYN=1, ACK=0)

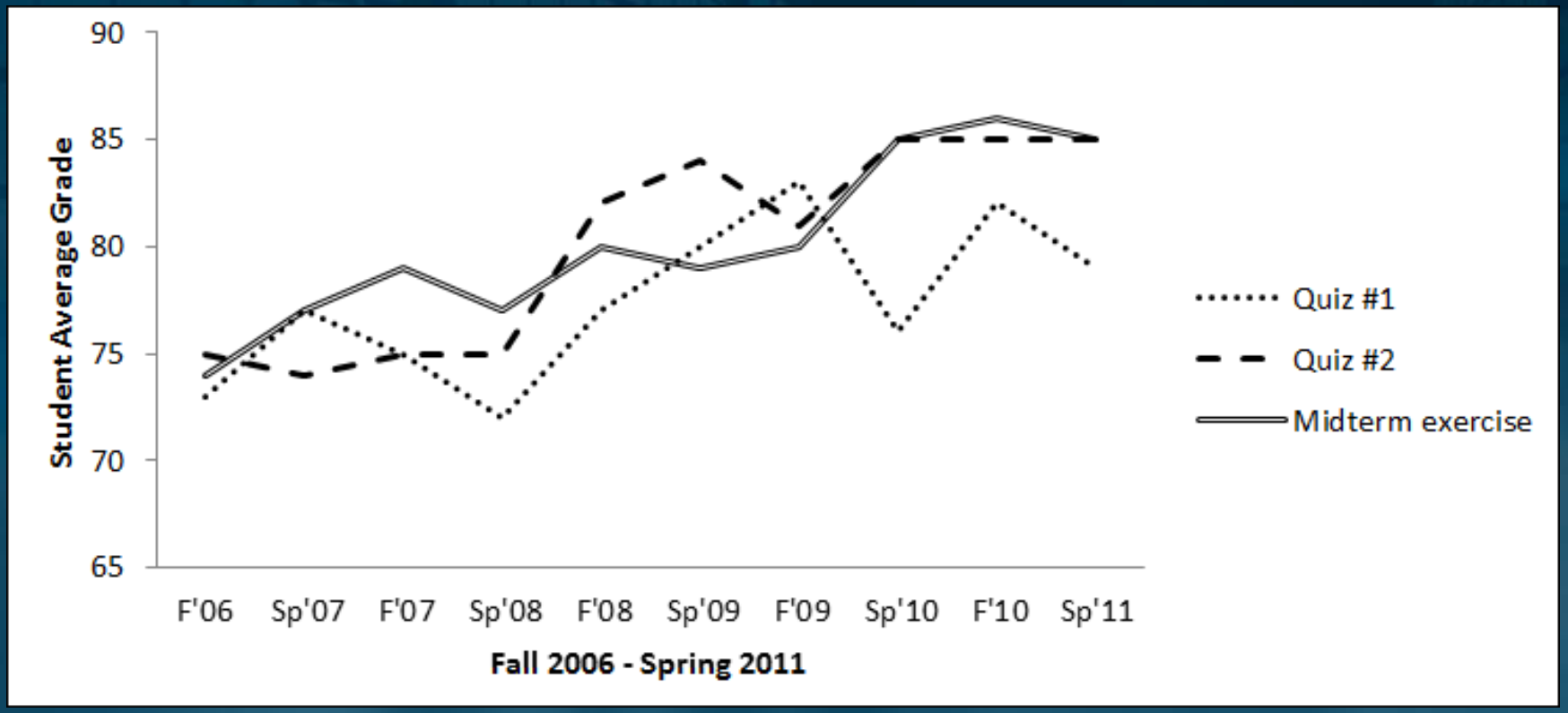
ICMP packets

Packet #6: (ICMP, Type = 8, Code = 0, Identifier = 100, Sequence number = 1)

Packet #7: (ICMP, Type = 0, Code = 0, Identifier = 100, Sequence number = 1)

Packet #8: (ICMP, Type = 0, Code = 0, Identifier = 200, Sequence number = 1)

Students' Grading Performance



The hands-on lab exercise allowed students to better anatomize the concept of stateless and stateful packet filtering learned from the lecture

Students' Satisfaction

To measure their satisfaction level and collect their feedback regarding the discussed hands-on lab exercise: An anonymous questionnaire was administered to 110 students, who participated in the lab exercise:

Questions	Responses
Did you enjoy the hands-on lab exercise?	• 86% strongly agree • 11% agree • 2% neither agree or disagree • 1% disagree
Do you think the hands-on lab exercise is easy to follow and straightforward?	• 85% strongly agree • 10% agree • 2% neither agree or disagree • 3% disagree
Do you feel you understand the theoretical concepts better after performing the hands-on lab exercise?	• 87% strongly agree • 9% agree • 3% neither agree or disagree • 1% disagree
How likely are you to recommend the hands-on lab exercise to others?	• 88% strongly agree • 9% agree • 2% neither agree or disagree • 1% disagree
Would you like to see similar hands-on lab exercises offered in your network security classes?	• 90% strongly agree • 8% agree • 1% neither agree or disagree • 1% disagree

Conclusion:

Information Security Program (Undergraduate)

Security concepts

Hands-on lab exercises

- **Better anatomize the concepts**
- **Hands-on skills**

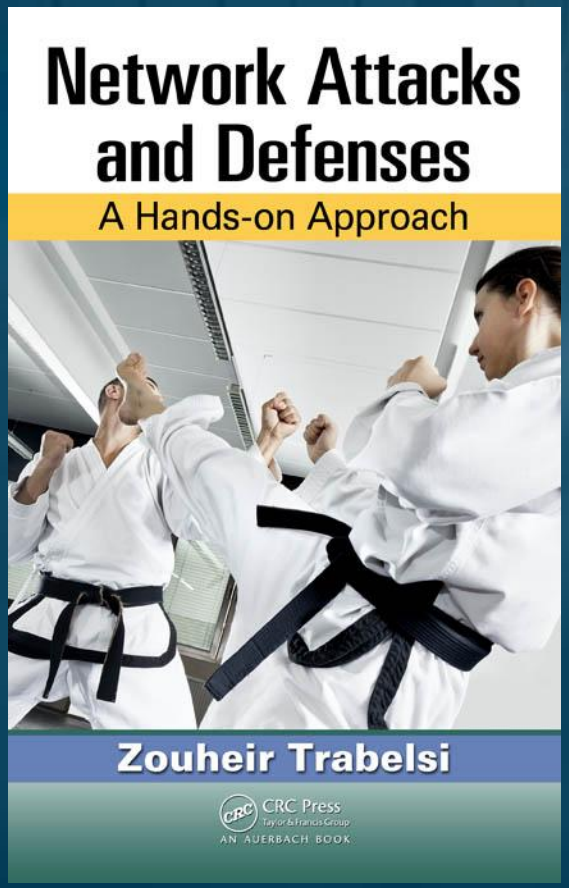
Information Security Program (Undergraduate)

Hands-on lab exercises about **defense** techniques

Hands-on lab exercises about **offensive** techniques (Ethical hacking)

Hands-on lab exercises about defense and offensive techniques

Textbook:



October 2012

Papers:

"Switch's CAM Table Poisoning Attack: Hands-on Lab Exercises for Network Security Education," Proceedings of the 14th Australasian Computing Education Conference (ACE 2012), Australia.

"Hands-on Lab Exercises Implementation of DoS and MiM Attacks using ARP Cache Poisoning", Proceedings of the Information Security Curriculum Development Conference 2011 (InfoSecCD 2011), USA.

"ARP Spoofing: A Comparative Study for Education Purposes", Proceedings of the Information Security Curriculum Development Conference (InfoSecCD 2009), USA.

Thank You

What Students Learn

Protect networks and systems from attacks

Computer Forensics

Filter traffic

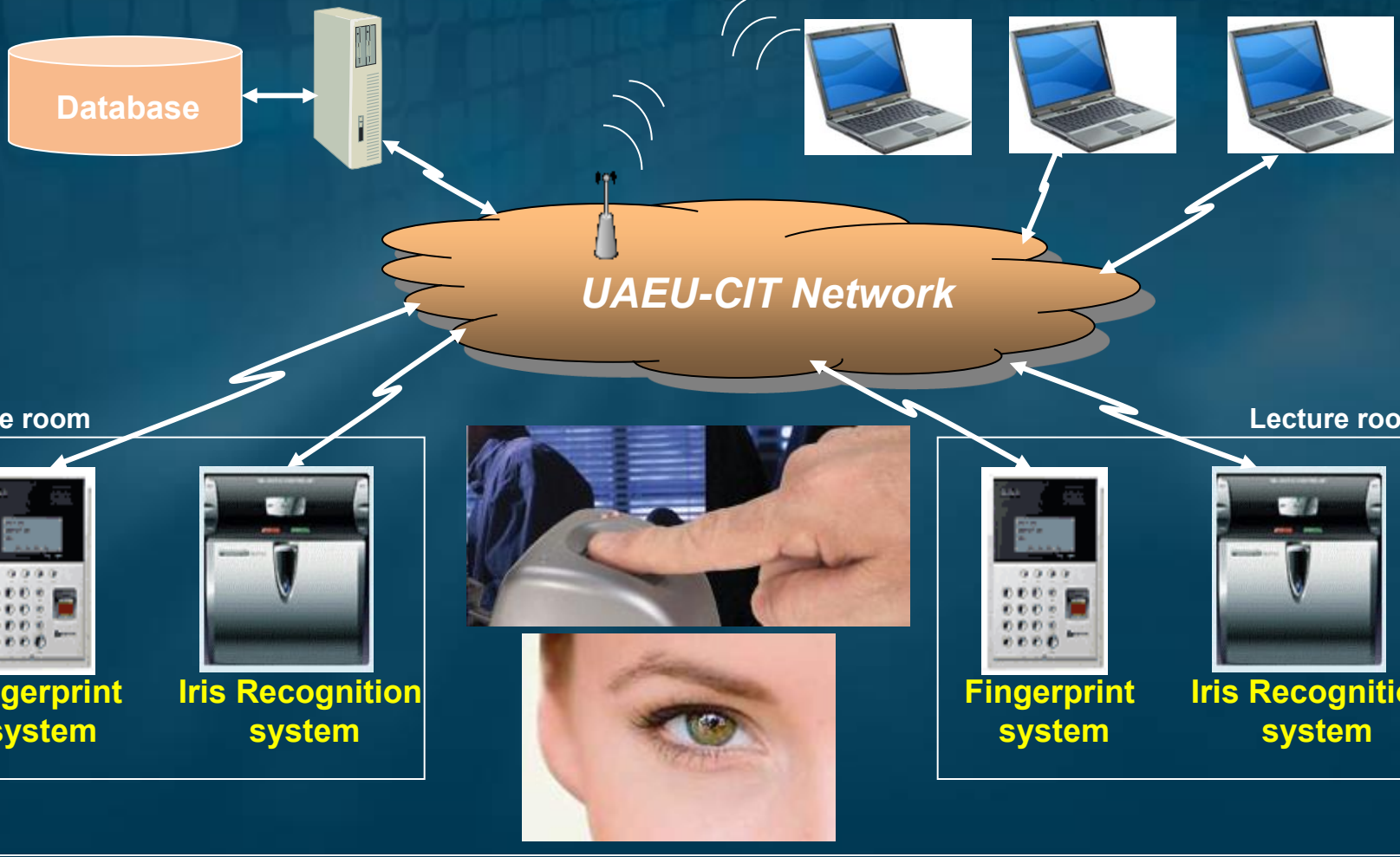
Implement biometrics solutions

Develop Virus and AntiVirus

Use and implement cryptography solutions

Security audit…

UAEU Biometrics e-Attendance System



The UAE Iris Expellees Tracking and Border Control System

64

Ethical Hacking, Penetration Testing, Computer Forensics Lab

Develop viruses

Cybercrime

Computer Forensics

Security auditing


Intrusion Detection System (IDS)

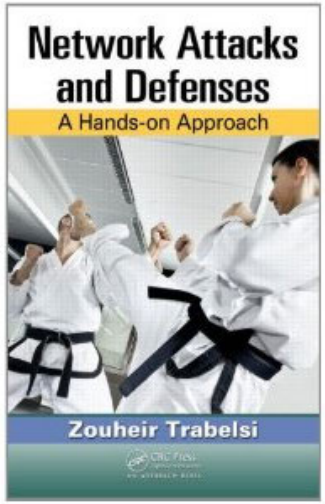
Textbook:

amazon

Your Amazon.com | Today's Deals | Gift Cards | Help

Shop by Department ▾ Search Books ▾

Books Advanced Search Browse Subjects New Releases Best Sellers The New York Times® Best Sellers Children's Books Textbooks Sell Your Book



Network Attacks and Defenses: A Hands-on Approach [Hardcover]

Zouheir Trabelsi (Author)

Like (0)

List Price: ~~$89.95~~

Price: $81.70 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $8.25 (9%)

Pre-order Price Guarantee. Learn more.

This title has not yet been released.

You may pre-order it now and we will deliver it to you when it arrives.

Ships from and sold by **Amazon.com**. Gift-wrap available.

Certification Central

Ace your tech certification test with resources from Certification Central. Get gu

from CCNA and SQL server to PMP and Network+. Explore more.

Product Details

Hardcover: 472 pages

Publisher: Auerbach Publications; 1 edition (October 22, 2012)

Language: English

ISBN-10: 1466517948

ISBN-13: 978-1466517943

Shipping Information: View shipping rates and policies

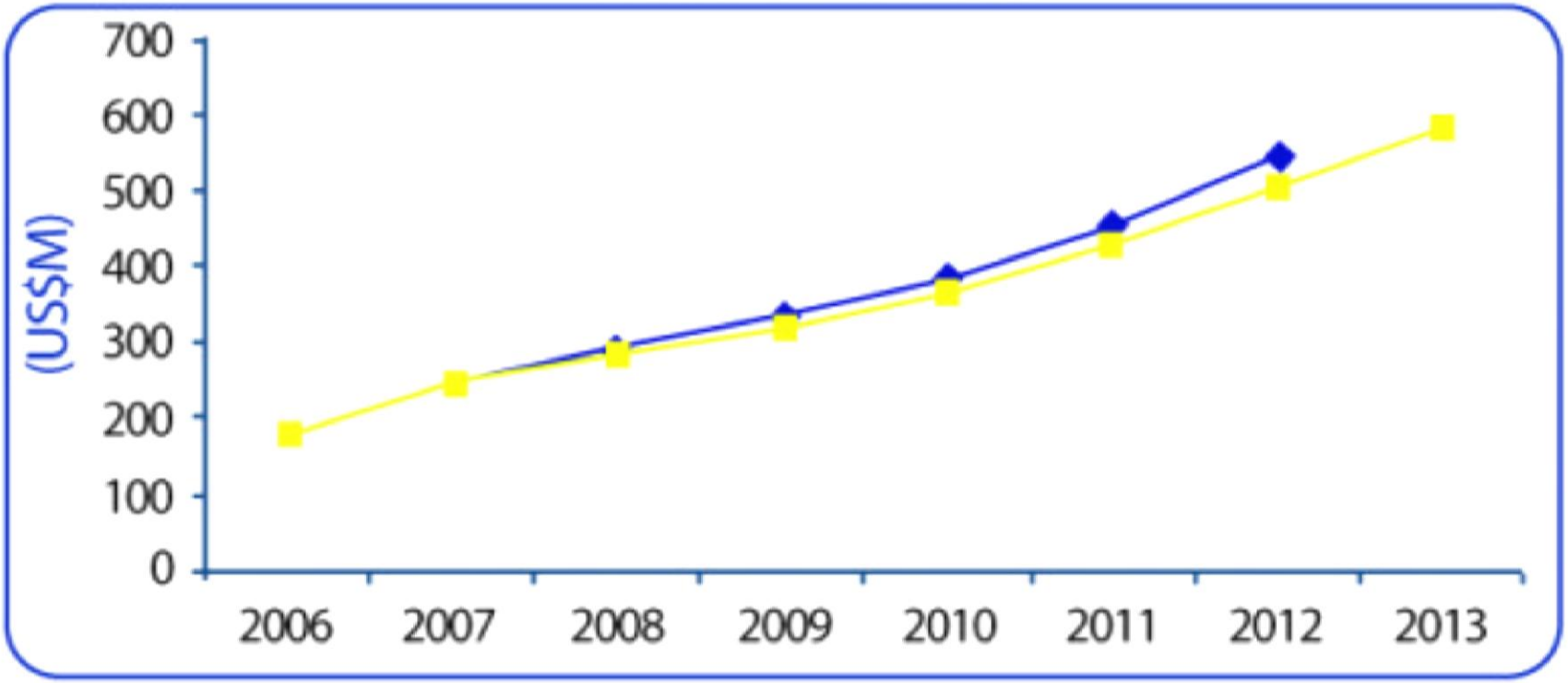
The UAE Iris Expellees Tracking and Border Control System

Dubai Airport

Abu Dhabi Int'l Airport T1

Forecasts of the Security Market in Gulf States

(KSA, UAE & OGCC)



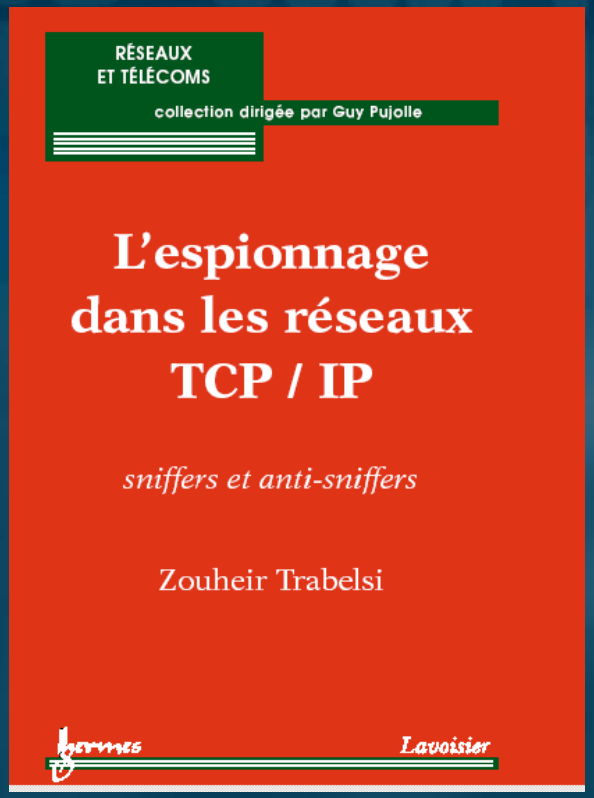
Huge investment in IT security by GCC countries

"IDC project that over the next five years, the IT security market in the Persian Gulf region will grow at an average annual rate of 23%."

"UAE was the second largest source of security expenditure in the region last year, with 31.2% share."

Security Experimental Facilities

Research Activities



Students Senior Projects
Students Security Course Project
Faculty Research Projects

Espionage in IP Networks:
Sniffers and AnitiSniffers

www.amozon.fr

Information Security Program

Security Labs

State-of-the-Art Security Labs

1 million US$

Intrusion Detection & Prevention Lab

Firewall & VPN Lab

Wireless Security Lab

Cryptography Lab

Biometrics


UAEU
Faculty of Information Technology

Information Security Program at UAEU

Cryptography

Firewall & VPN

Intrusion Detection and Prevention (IDS/IPS)

Database security

OS security

Biometrics

Virus & Malicious Code

Web application security

Network Traffic Analysis

Ethical Hacking

Secure e-transactions

Wireless Security

Security Auditing, Penetration testing

Intrusion Detection & Prevention Lab

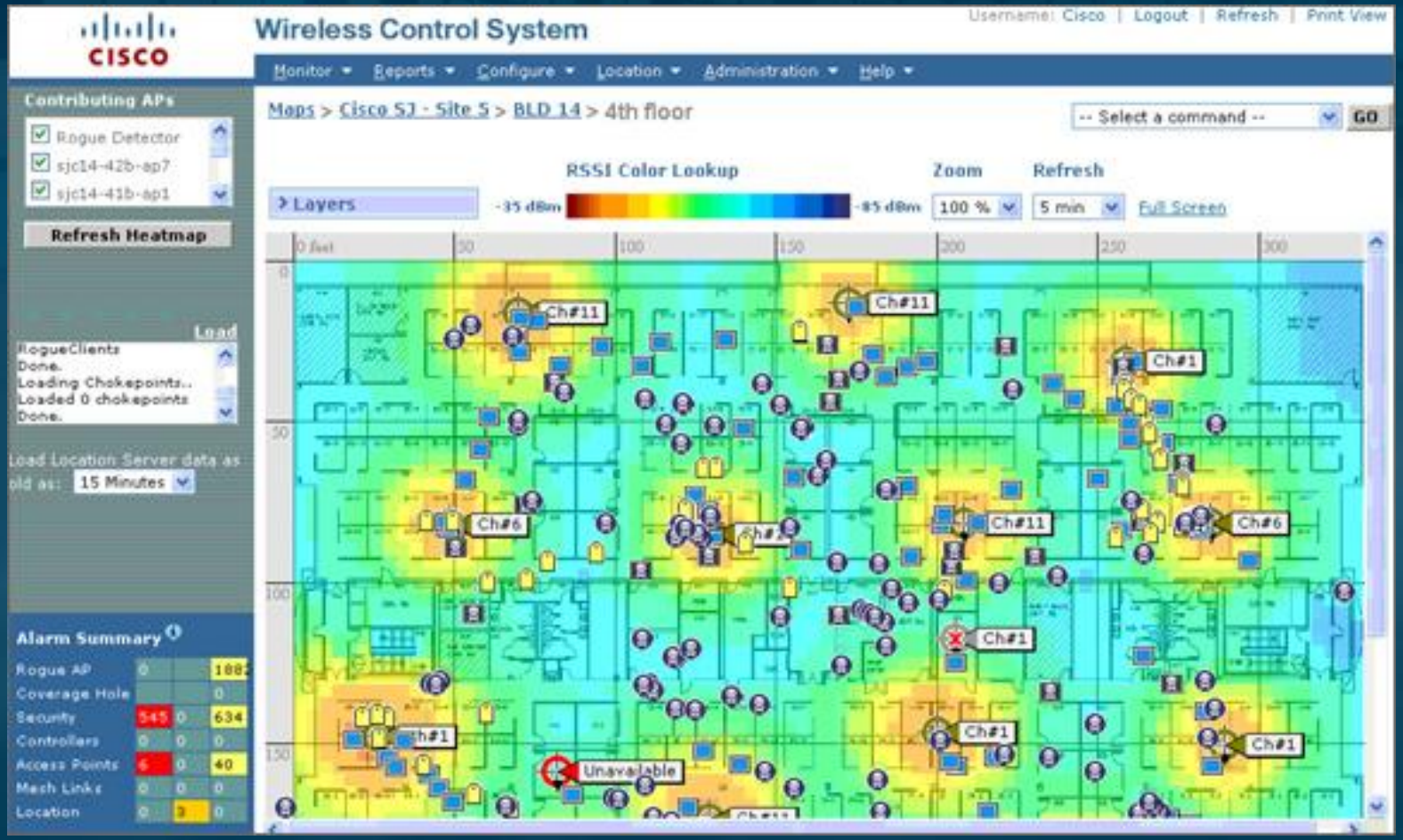
Cisco Switch 3560 Series

Dynamic ARP Inspection:

- ARP cache poisoning attack
- MiM attack
- DoS attack
- Switch CAM table poisoning

Routers

Wireless Tracking System



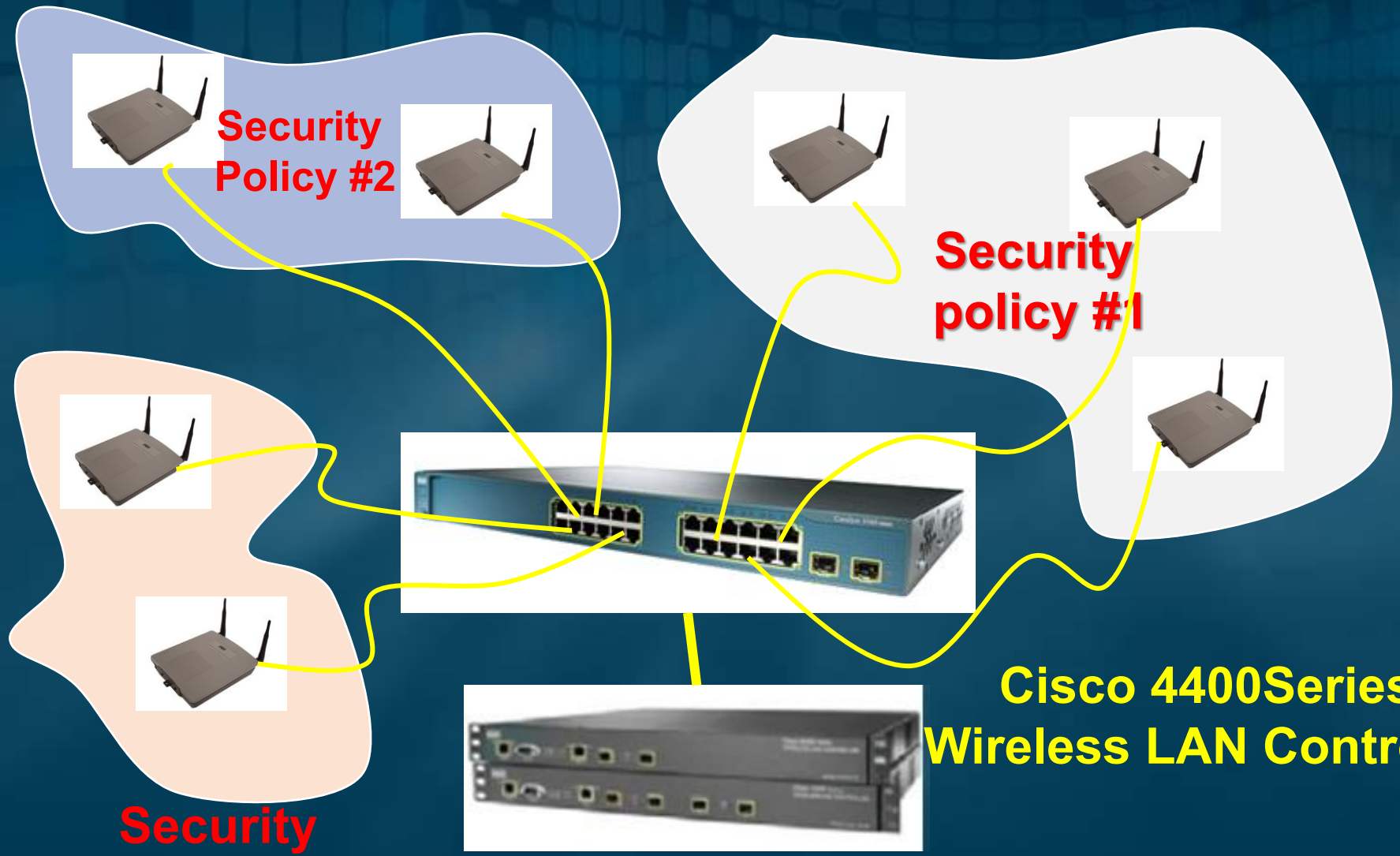
Information Security Program (Undergraduate)

Security concepts

Hands-on lab exercises

- Better anatomize the concepts
- Hands-on skills

Wireless Security Lab



Stateless and Stateful Firewall

A **stateless** firewall has:

No mechanism to identify packets that belong to established sessions