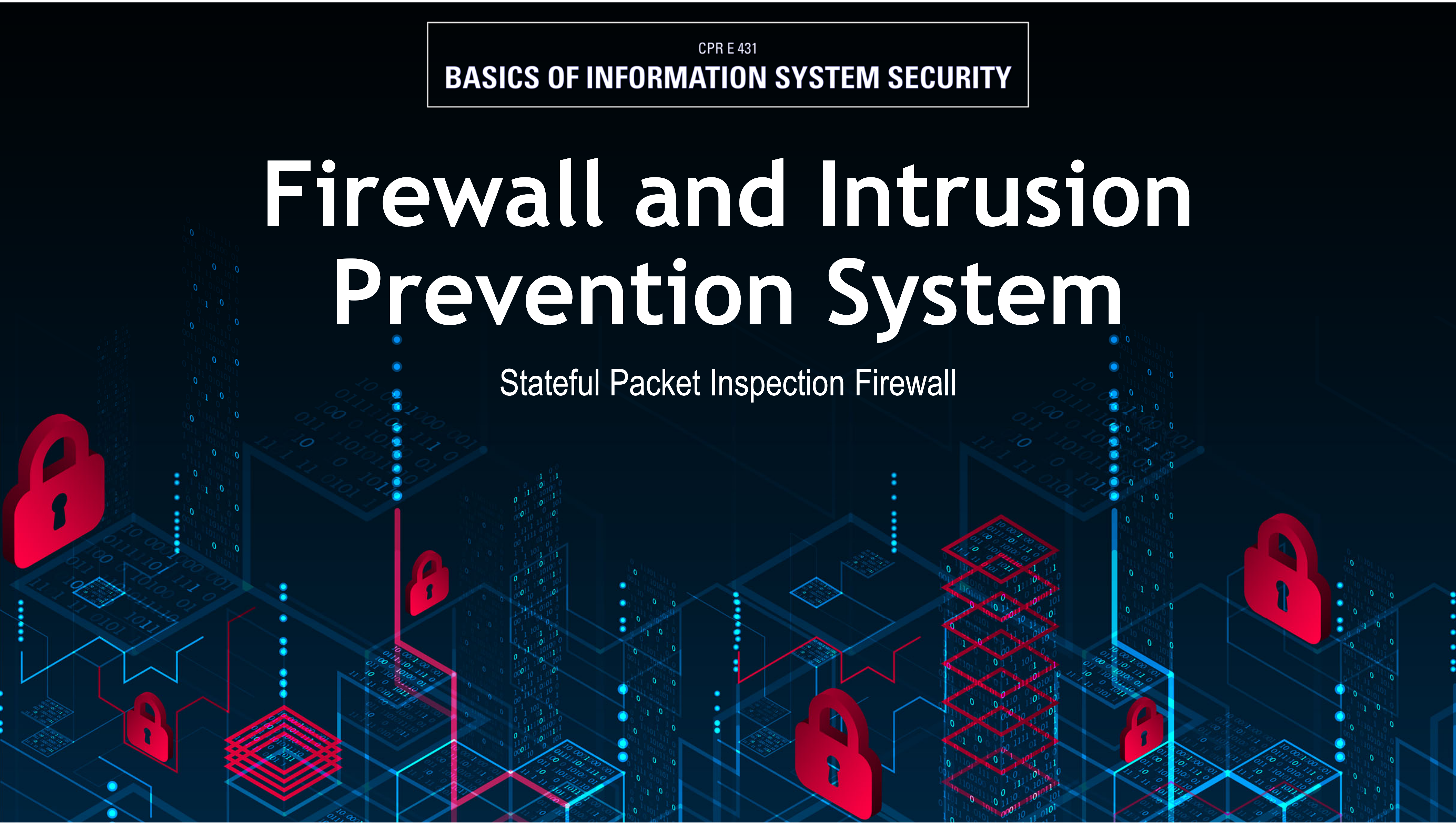


CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Firewall and Intrusion Prevention System

Stateful Packet Inspection Firewall

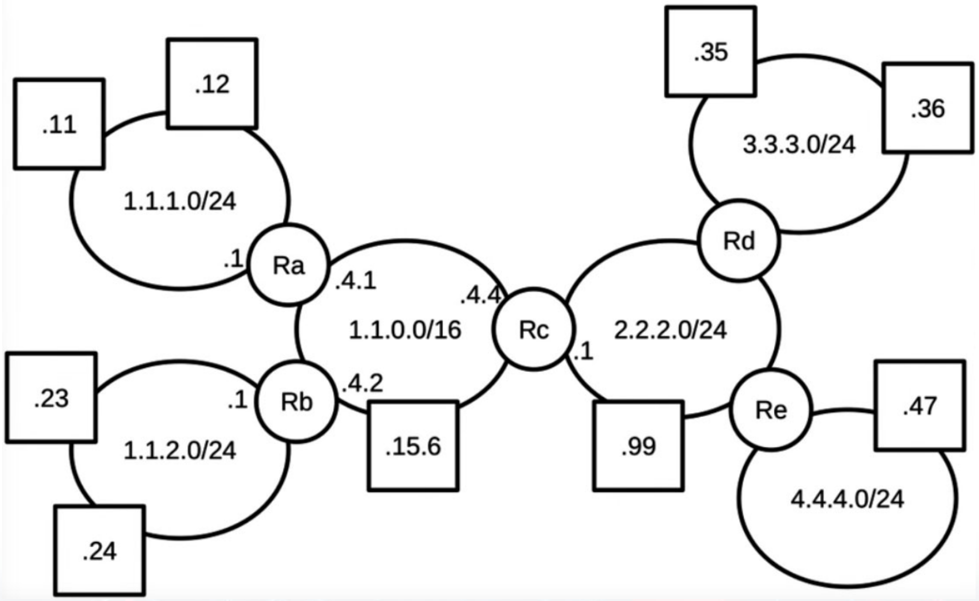
Video Summary

- A Drawback of Packet Filtering Firewall
- Stateful Packet Inspection Firewall
- Example Network
- Connection State Table

Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra
Aim: Stop everyone except 1.1.1.12 from browsing to servers on 3.3.3.0/24

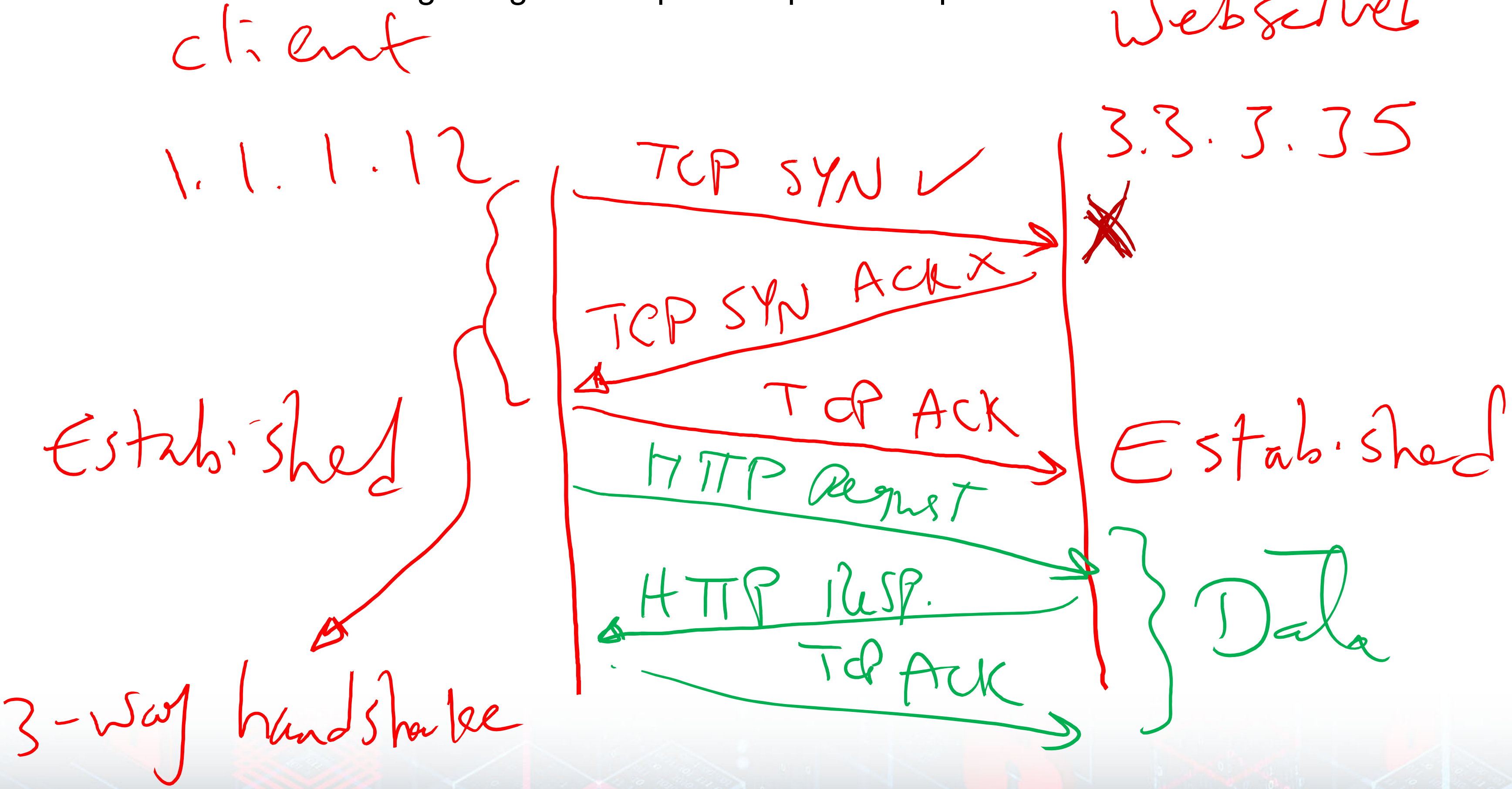
SrcIP	DstIP	SrcPort	DstPort	Protocol	Action
.12	3.3.3.0/24	*	80	6	Allow



Default
Drop.

TCP/Webserver

Browsing using TCP request/response sequence



Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra
Aim: Stop everyone except 1.1.1.12 from browsing to servers on 3.3.3.0/24

Is 1.1.1.12 able to communicate with the server successfully?

No

How we can resolve this issue?

	SrcIP	DstIP	SrcPort	DstPort	Protocol	Action
①	.12	3.3.3.0/24	*	80	6	Allow
②	3.3.3.0/24	.12	80	*	6	Allow
→	3.3.3.36	.12	80	40981	6	Allow

Example Network

What other problem we have here? Can an attacker reach 1.1.1.12? What about using 3.3.3.36 to send attack 1.1.1.12?

Yes

How to stop that?

???

stateful Packet inspecton firewall.

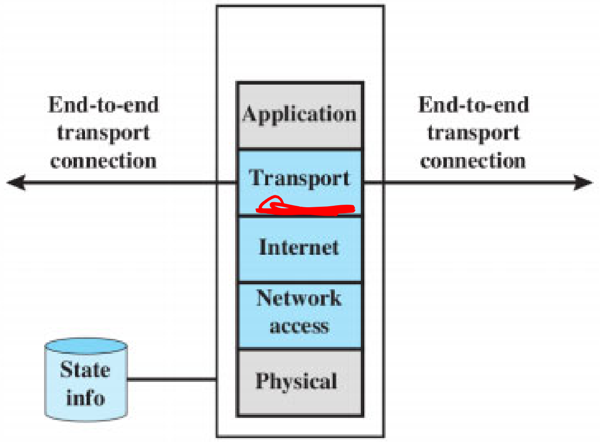
Stateful Packet Inspection

- Traditional packet filtering firewall makes decisions based on individual packets; don't consider past packets (stateless)
- Many applications establish a connection between client/server; group of packets belong to a connection
- Often easier to define rules for connections, rather than individual packets
- Need to store information about past behaviour (stateful)
- Stateful Packet Inspection (SPI) is extension of traditional packet filtering firewalls
- Issues: extra overhead required for maintaining state information

3-way handshake

Stateful Packet Inspection

- For connections accepted by packet filtering firewall, record connection information
  - src/dest IP address, src/dest port, sequence numbers, connection state (e.g. Established, Closing)
- Packets arriving that belong to existing connections can be accepted without processing by firewall rules


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
State info
End-to-end transport connection

Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra

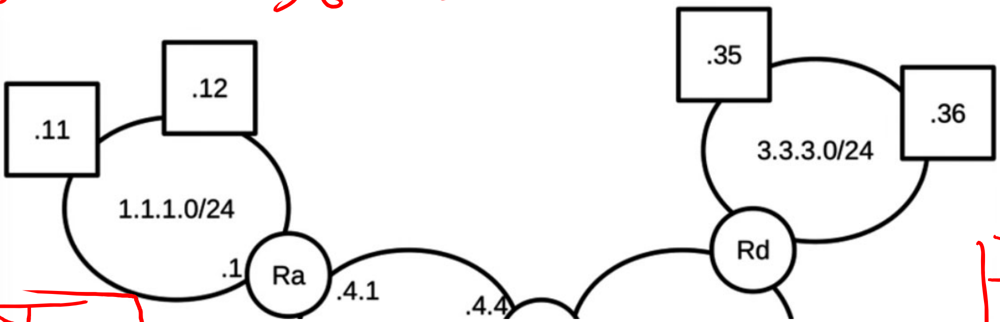
Aim: Stop everyone except 1.1.1.12 from browsing to servers on 3.3.3.36

FW Table

Src	Dst	Protocol	Action
1.1.1.12 : 40981	3.3.3.36 : 80	6	Allow

SPI Table

Src	Dst	Protocol	State
.12 : 40981	.36 : 80	6	~~SYN~~ ~~SYN ACK~~ Established



IP	TCP	Data

IP	TCP	Data

SrcIP: .12 SrcP: 40981

Dst: .36 DstP: 80

Port: 6 Flag: SYN

SrcIP: .36 SrcP: 80

Dst: .12 DstP: 40981

Port: 6 Flag: SYN ACK

Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Video Summary

- A Drawback of Packet Filtering Firewall
- Stateful Packet Inspection Firewall
- Example Network
- Connection State Table