RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Become a Certified Professional in IPv6 Security

RIPE NCC Open House

RIPE NCC Learning & Development | 20 October 2021 | RIPE NCC Open house

Inspiration

Why are we doing this?

- Our Mission: “As a neutral source of information and knowledge, we actively contribute to a stable and innovative Internet”
- RIPE NCC is a non-for profit, neutral, impartial and self-sufficient membership

Training and Education Services

Online Learning	Face-to-Face Training
Academy	Training Courses
Webinars	Tutorials
Educa	Course Material
Videos	

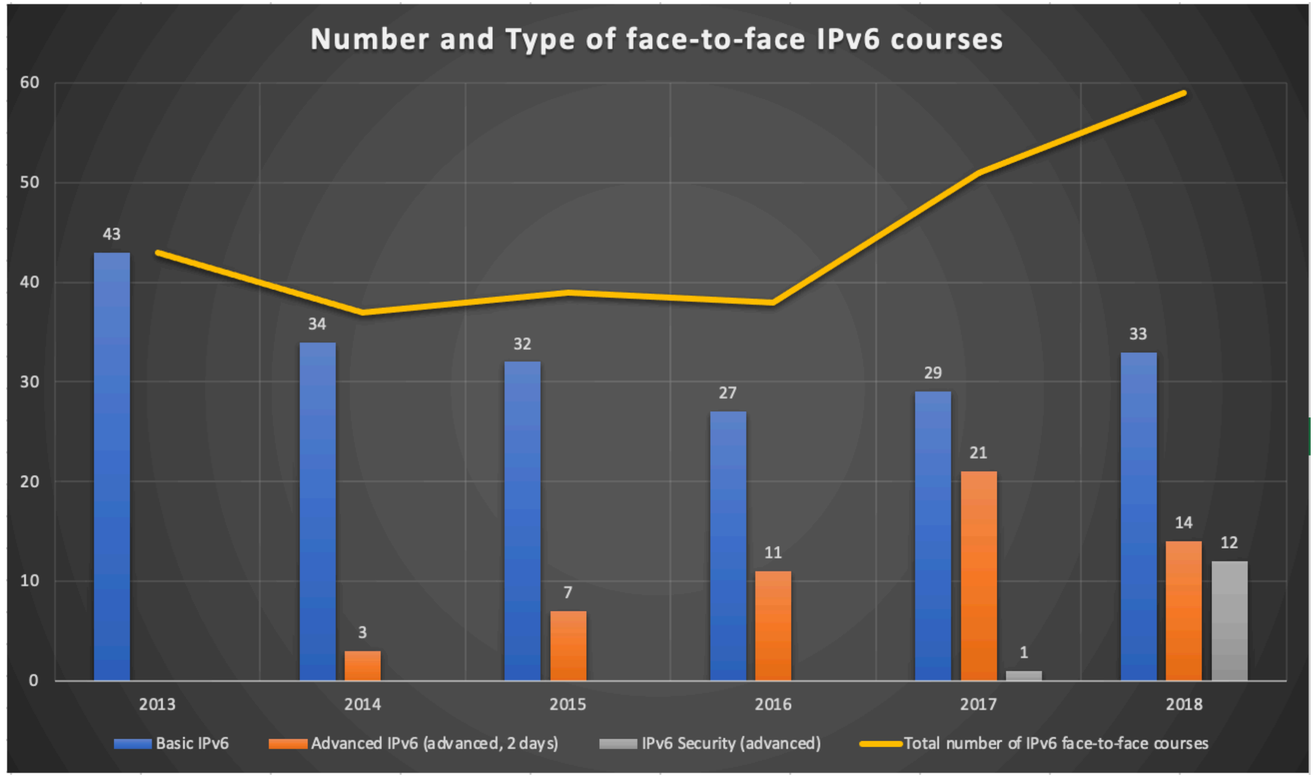
https://www.ripe.net/training

RIPE NCC Certified Professionals

https://www.ripe.net/certified-professionals

Why IPv6 Security?

- RIPE Community:
  - 2016 and 2019 survey results asked for more IPv6, more security, more training
- Internal knowledge and goals:
  - IPv6 use will keep growing
  - The Internet should be as secure as possible
- That led us to define **IPv6 security as a topic in demand**



How are we doing it?

- **In-person course** for members (slides available to all),
- Three **webinars** for members (recordings and slides available to all)
- NEW: An **e-learning course** available to all, and for free

https://academy.ripe.net/ipv6-security

Content Approach

We decided to…

Broad range of topics

- Starting point to continue learning in the future
- Includes many references
- How to find relevant information even after the course

Advanced course
Prior knowledge needed

- Networking basics, IPv4
- IPv6 (IPv6 Fundamentals from the RIPE NCC Academy)
- General network security knowledge

Who should take it

- Network Engineers, Network Architects, Network Designers
- Security Engineers, Information Security Officer
- Helpdesk/Support, Consultants

Network Security a big topic. We focus on …

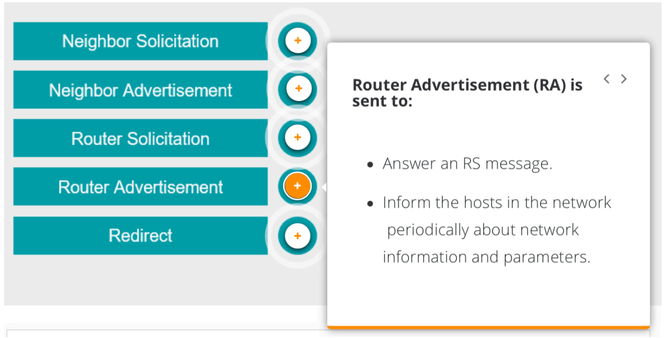
Layer 3 / IPv6

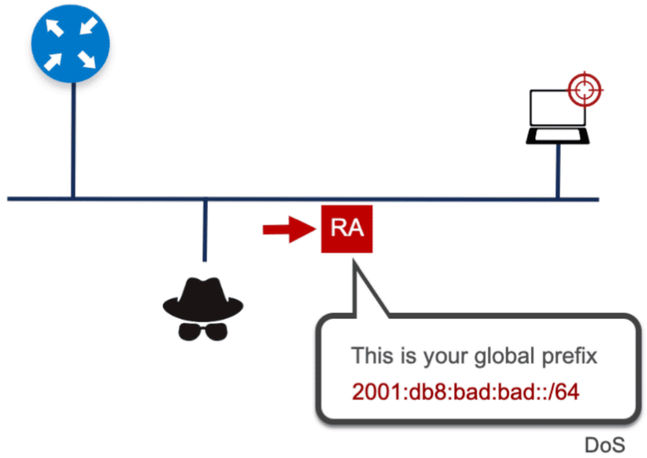
Not Layer 2, transport or application layers security

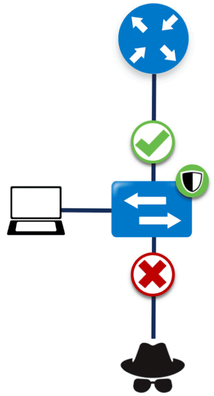
New IPv6-related security topics

IPv4 security is helpful, but… What's new with IPv6?

Learn - Threat - Solution (and Scenario)

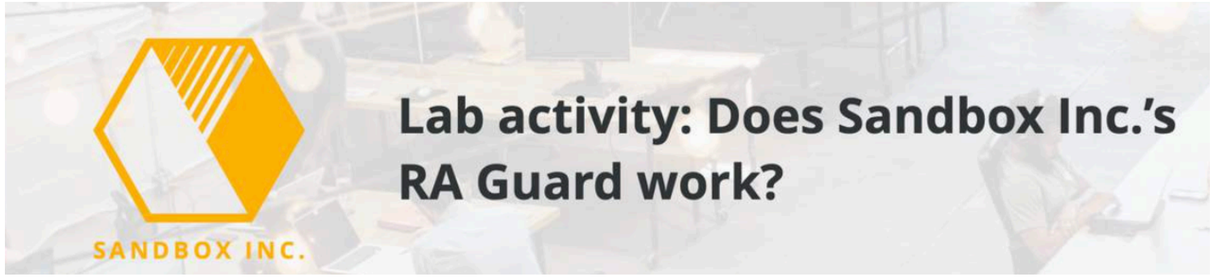






There are two ways of implementing RA-GUARD:

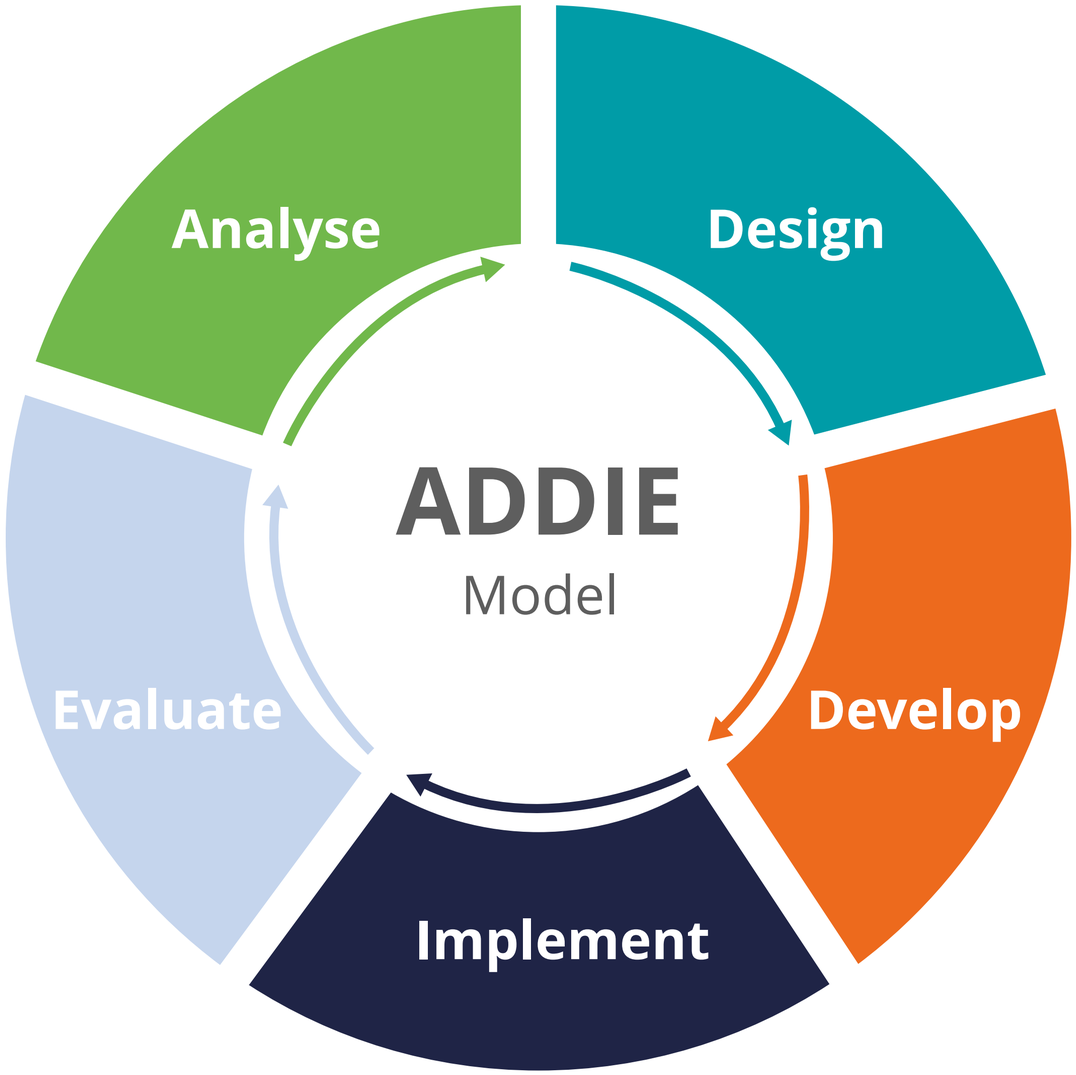
- **Stateless RA-Guard:** Decisions are based on examination of received RA message or in the switch static configuration.
- **Stateful RA-Guard:** The switch first learns dynamically where the router is and then allows RAs to be received from authorised sources learned in that period.



Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Introduction	**Basic IPv6 Protocol**	**Protocols associated with IPv6**	**Internet-wide IPv6 Security**	**High Level Strategy**
	Basic Header	ICMPv6	**IPv6 Traffic Filtering**	
	Extension Headers	**NDP**	DDoS	
	IPsec	**MLD**	Transition Mechanisms	
	Addressing Architecture	DNS	BGP Routing	
		DHCPv6		
		Routing Protocols		
Lab installation	2 Lab activities	3 Lab activities	1 Lab activity	

Learning Methodology

Course Design Model



Our Learning Methodology (simplified)

How does this help the learner?

Our Process

Our Process

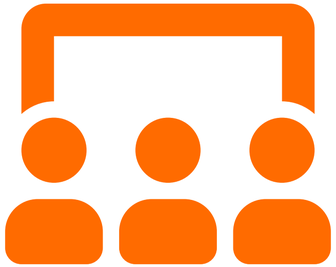
Research

- Current best practices
- Surveys
- Expert feedback

Our Process

Research

- Current best practices
- Surveys
- Expert feedback



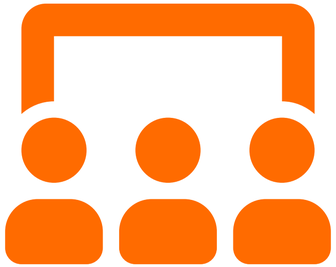
Team

- Subject matter experts
- Technical specialists
- Visual designers
- Education professionals

Our Process

Research

- Current best practices
- Surveys
- Expert feedback



Team

- Subject matter experts
- Technical specialists
- Visual designers
- Education professionals

Develop

- Lessons, diagrams, animations
- References & job aids
- Labs & Exercises
- High level strategy

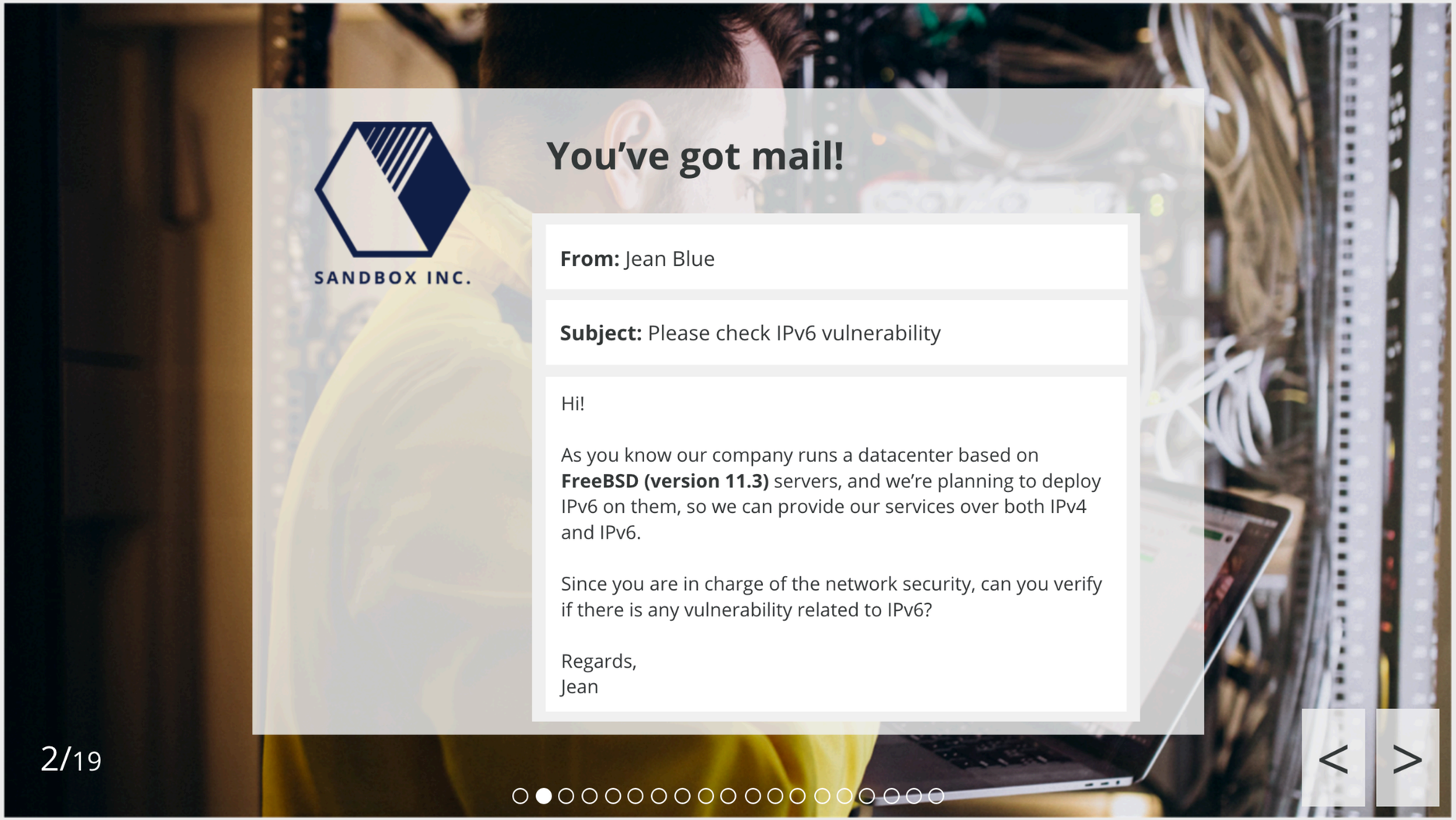
Examples

References and Job-Aids

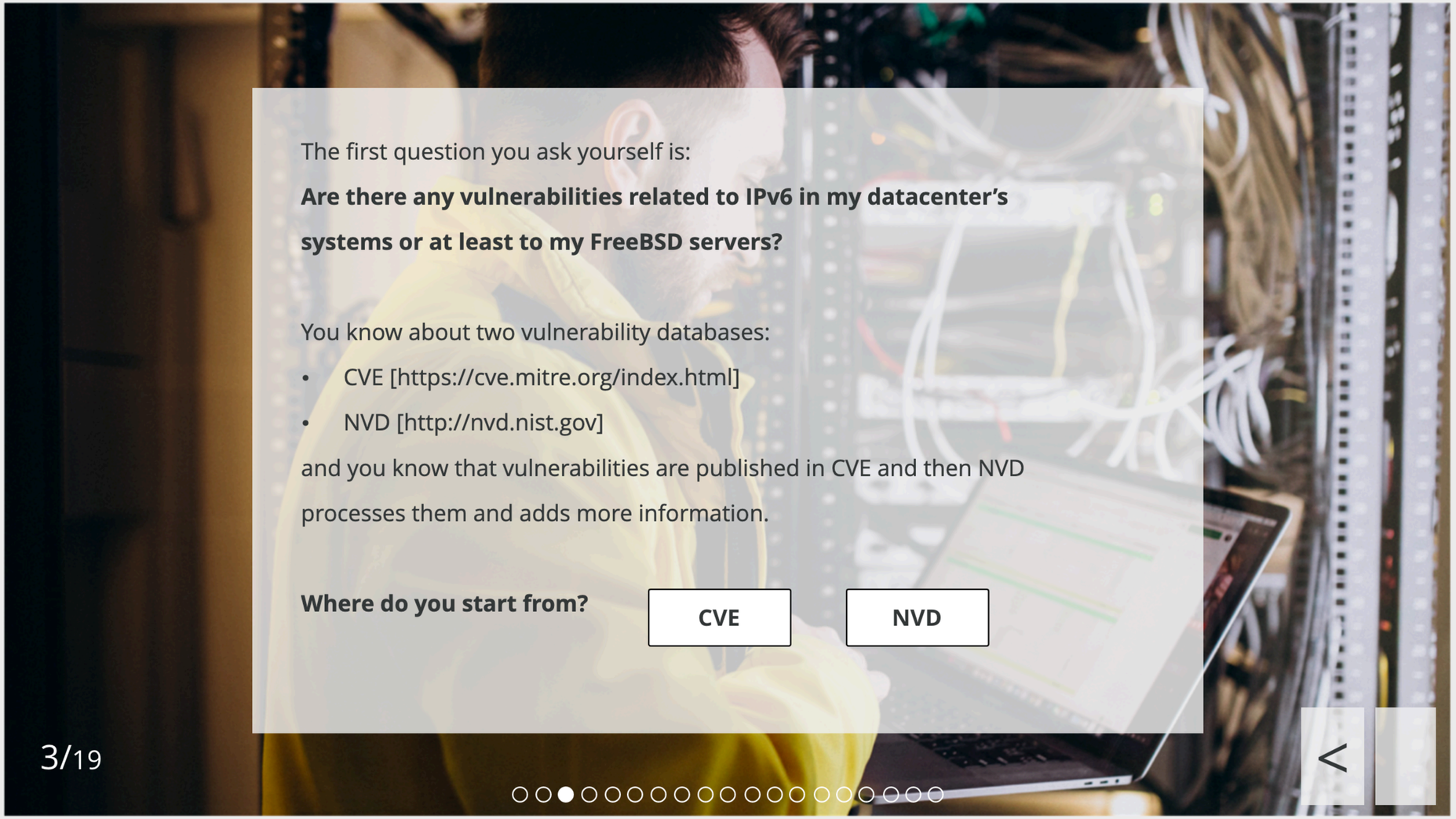
Information category	**Standardisation Bodies**	**Vulnerabilities Databases**	**Security Tools**	**Cybersecurity Organisations**	**Vendors**	**Public Forums**
Sub-categories	IETF		Vulnerability Scanners	CSIRTs / CERTs Gov. / LEAs		Mailing Lists Groups of Interest Security Events
Information in this category	Security considerations Protocol updates Security recommendations	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds Affected devices in your network	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds “0 Day” vulnerabilities	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds “0 Day” vulnerabilities	“0 Day” vulnerabilities News Trends Lessons learned
Examples	RFCs, I-Ds	NVD, CVE	OpenVAS	CERT-EU ENISA EUROPOL/EC3	Cisco, Juniper, MS, Kaspersky, etc.	NOGs, IETF, IPv6 Hackers, Reddit, Troopers, etc.

IPsec in TRANSPORT MODE

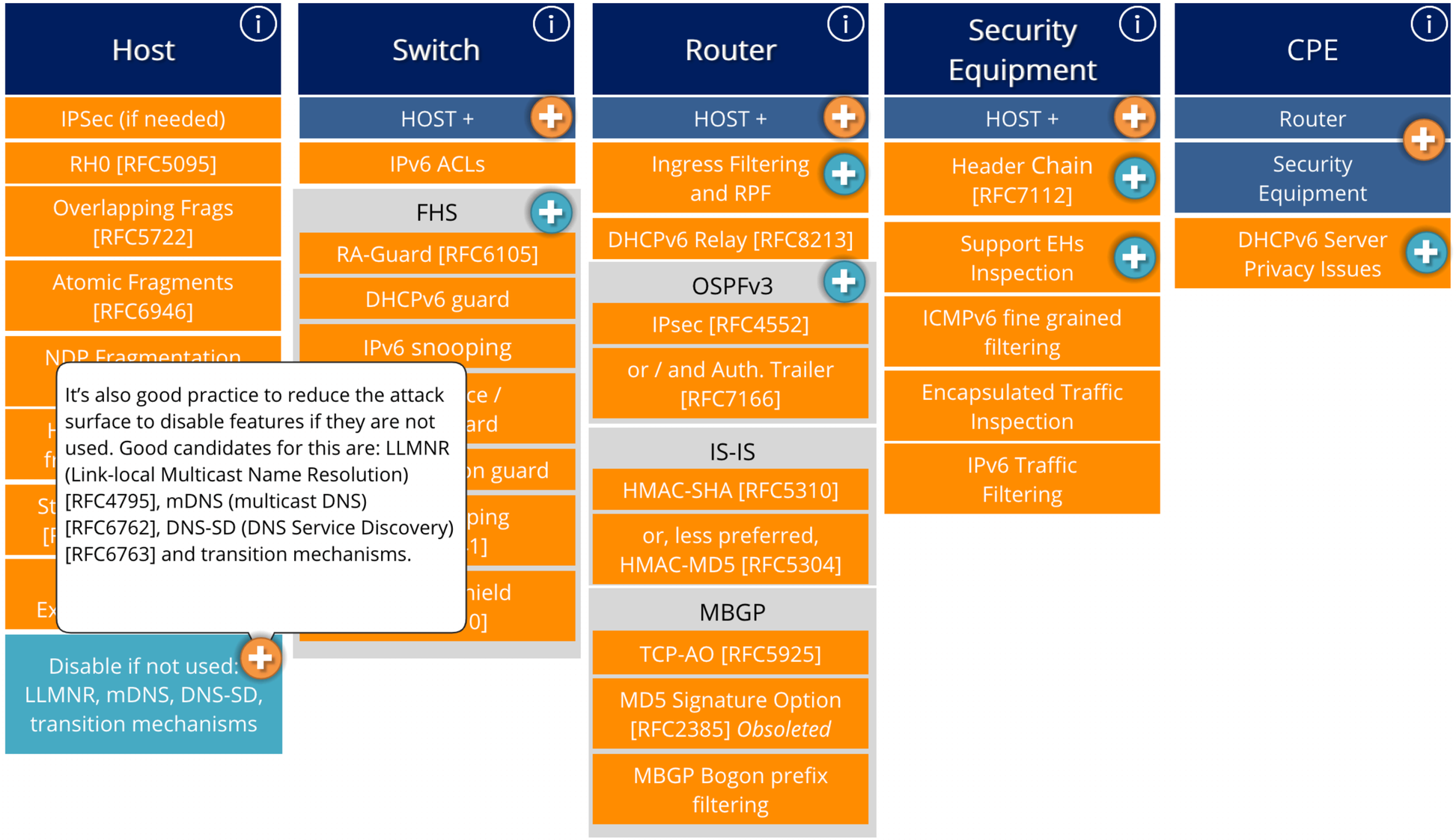
Scenarios / Exercises / Labs



Scenarios / Exercises / Labs



Developing a High-Level Security Strategy



Labs