IPv6 Security

Exam Guide

IPv6 Security - Exam Guide

The IPv6 Security exam is intended for individuals capable of designing a high-level strategy to protect an IPv6 network against common threats

Recommended Knowledge:

- IPv4 and IPv6 networking knowledge (IPv6 at the level of the IPv6 Fundamentals – Analyst Exam)
- Knowledge about the most common IP network security concepts
- Proficiency with details of IPv6 and associated protocols like ICMPv6, NDP, MLD and DHCPv6
- Ability to describe common IPv6 security threats and available mitigation techniques
- Familiarity with IP traffic filtering concepts
- General knowledge about existing routing protocols, and more specifically about BGP
- Experience with security assessment tools
- Experience with information security search from common public sources

Exam Structure:

Each LIR receives three exam vouchers per year. Registered LIR contacts can claim these vouchers in the RIPE NCC Academy Dashboard.

The exam validates the ability to:

- Justify the need for implementing IPv6 security solutions
- Plan how to protect your IPv6 network against new attack vectors and most common threats
- Design filtering rules for IPv6 packets
- Choose security options for IPv6 routing protocols
- Choose the correct type of tool to assess IPv6 security threats and mitigation techniques
- Make use of up-to-date information about IPv6 network vulnerabilities and mitigation techniques
- Design a high-level IPv6 security strategy

50
Number of questions

60
minutes
Time limit

70
Passing score

Types of Questions

The exam contains different types of questions:

Multiple choice: Has one correct response and three incorrect responses.
Multiple response: Has two or more correct responses out of five or more alternatives.
Matching: Contains a list of items or statements that must be correctly matched to another list of items or statements.
Drag and drop: Drag words or images into gaps in a paragraph of text or a base image.
Fill in the blank: A question or sentence in which a blank line needs to be replaced with the missing word or phrase.

Unanswered questions are scored as incorrect.

Unscored Items:

The exam may contain items that are included in the exam to trial run new exam questions for other RIPE NCC certifications. These items are not identified and will not count towards your score. Only the scored items are worth 100% of your score.

Exam Content Distribution:

Domain	Percent of Exam
IPv6 Security Strategy, Tools, and Information	16%
Basic IPv6 Protocol Security	24%
Security of Protocols Associated With IPv6	36%
Internet-Wide IPv6 Security	24%

How can you study for the exam?

E-learning course

Taking our free online self-paced IPv6 Security e-learning course in the RIPE NCC Academy is the best way to prepare yourself for the IPv6 Security exam. The course consists of seventeen modules and seven lab activities and takes you about twenty four hours to complete.

- Covers all exam knowledge and skills
- Available for free

Go to the RIPE NCC Academy

Face-to-face training course

RIPE NCC members can attend an in-person IPv6 Security training course. We offer courses throughout our service region, and attending a course is a great way to learn directly from our trainers and your peers.

- Partially covers exam knowledge and skills
- Courses for members only

Register for a face-to-face course

Webinars

We also offer several live online webinars on IPv6-related topics, such as addressing plans and filtering. This is an easy way to interact directly with our trainers and ask them your questions!

- Partially covers exam knowledge and skills
- Live webinars are available to all

Register for a webinar

Exam Outline

To pass the exam, you must possess the minimum level of knowledge, skills and abilities in understanding and performing the following:

1. IPv6 Security Strategy, Tools, and Information

1.1 The need for IPv6 security

1.1.1 Provide reasons that support the need for IPv6 security

1.1.2 Provide reasons that support the need for continually updated knowledge on IPv6 security

1.2. High level IPv6 security strategy

1.2.1 Propose IPv6 security solutions for the relevant parts of the network for ISPs, data centers, and enterprise

1.2.2 Match IPv6 security features with each type of IPv6 network device

1.2.3 Choosing security measures for an IPv6 security strategy considering the IPv6 security course guidelines

1.3. Up-to-date tools and information about IPv6 security threats and mitigation techniques

1.3.1 Choose the correct tool to assess IPv6 security threats and mitigation techniques

1.3.2 Identify the common information sources and the type(s) of information they contain related to IPv6 network vulnerabilities and mitigation techniques

1.3.3 Choose relevant information from a common information source to protect an IPv6 network

2. Basic IPv6 Protocol Security

2.1 Basic IPv6 protocol security threats

2.1.1 Identify the IPv6 security related fields of the IPv6 basic header

2.1.2 Identify the IPv6 security threats related to the IPv6 basic header

2.1.3 dentify the IPv6 security aspects of the IPv6 extension headers

2.1.4 Identify the IPv6 security threats related to IPv6 extension headers

2.1.5 Identify the IPv6 security aspects of the IPv6 addressing architecture

2.1.6 Identify the IPv6 security threats related to the IPv6 addressing architecture

2.2 Security measures to protect from Basic IPv6 protocol security threats

2.2.1 Choose a suitable and available security measure for IPv6 security threats related to the IPv6 basic header

2.2.2 Choose a suitable and available security measure for IPv6 security threats related to the IPv6 extension headers

2.2.3 Choose a suitable and available security measure for IPv6 security threats related to the IPv6 addressing architecture

2.2.4 Identify the IPsec elements used by IPv6 to offer security in the IP layer

2.2.5 Choose the IPsec security protocol that offers the needed security

2.2.6 Choose the IPsec mode that best fits your security needs

Exam Outline

3. Security of Protocols Associated With IPv6

3.1 Security threats of protocols associated with IPv6

3.1.1 Identify the IPv6 security aspects of ICMPv6

3.1.2 Identify the IPv6 security threats related to ICMPv6

3.1.3 Identify the IPv6 security aspects of NDP

3.1.4 Identify the IPv6 security threats related to NDP

3.1.5 Identify the IPv6 security aspects of MLD

3.1.6 Identify the IPv6 security threats related to MLD

3.1.7 Identify the IPv6 security aspects of DNS

3.1.8 Identify the IPv6 security threats related to DNS

3.1.9 Identify the IPv6 security aspects of DHCPv6

3.1.10 Identify the IPv6 security threats related to DHCPv6

3.2 Security measures to protect from IPv6 associated protocol security threats

3.2.1 Choose a suitable and available security measure for IPv6 security issues related with ICMPv6

3.2.2 Choose a suitable and available security measure for IPv6 security issues related with NDP

3.2.3 Choose a suitable and available security measure for IPv6 security issues related with MLD

3.2.4 Choose a suitable and available security measure for IPv6 security issues related with DNS

3.2.5 Choose a suitable and available security measure for IPv6 security issues related with DHCPv6

4. Internet-Wide IPv6 Security

4.1 Internet-wide IPv6 security threats

4.1.1 Identify how Internet-wide IPv6 security threats could result in a DDoS attack or BGP hijack

4.1.2 Match IPv6 security threats with the correct category of IPv6 Transition Mechanism

4.2 Security measures to protect from Internet-wide IPv6 security threats

4.2.1 Identify security measures to protect from IPv6 BGP Hijacking

4.2.2 Describe MANRS Actions that have an impact on IPv6 network security

4.2.3 Write basic rules and recommendations about IPv6 BGP Bogon Prefix Filtering

4.2.4 Match security measures with the correct threat and associated category of IPv6 Transition Mechanism

Exam Outline

4.3 Filtering rules for IPv6 packets

4.3.1 Differentiate between two types of IPv6 filtering: packet forwarding vs. routing information

4.3.2 Choose filtering rules and recommendations for IPv6 packet filtering in order to improve the security of an IPv6 network

4.4 Available security options for IPv6 routing protocols

4.4.1 Choose the security options defined in the RIPng protocol standard

4.4.2 Choose the security options defined in the OSPFv3 standard

4.4.3 Choose the security options defined in the IS-IS standard

4.4.4 Choose the security options defined in the MBGP standard

Learning Resources

1. IPv6 Security Strategy, Tools, and Information

1.1 The need for IPv6 security

	RIPE NCC Academy IPv6 Security [16 hours]	**Training Course** IPv6 Security [1 day]	**Webinar** Basic IPv6 Protocol Security [2 hours]	**Webinar** IPv6 Associated Protocols Security [2 hours]	**Webinar** IPv6 Security Myths, Filtering and Tips [2 hours]
1.1.1 Provide reasons that support the need for IPv6 security	Module 1	Yes			Yes
1.1.2 Provide reasons that support the need for continually updated knowledge on IPv6 security	Module 1	Yes			Yes

1.2 High level IPv6 security strategy

1.2.1 Propose IPv6 security solutions for the relevant parts of the network for ISPs, data centers, and enterprise	Module 5.1	Yes			Yes
1.2.2 Match IPv6 security features with each type of IPv6 network device	Module 5.1	Yes			Yes
1.2.3 Choosing security measures for an IPv6 security strategy considering the IPv6 security course guidelines	Modules 1 & 5.1	Yes			

1.3 Up-to-date tools and information about IPv6 security threats and mitigation techniques

1.3.1 Choose the correct tool to assess IPv6 security threats and mitigation techniques	Module 5.2	Yes	Partially/Demo	Partially/Demo	Yes
1.3.2 Identify the common information sources and the type(s) of information they contain related to IPv6 network vulnerabilities and mitigation techniques	Module 5.2	Yes			Yes
1.3.3 Choose relevant information from a common information source to protect an IPv6 network	Module 5.2	Yes			Yes

Learning Resources

2. Basic IPv6 Protocol Security

2.1 Basic IPv6 protocol security threats

	RIPE NCC Academy IPv6 Security [16 hours]	**Training Course** IPv6 Security [1 day]	**Webinar** Basic IPv6 Protocol Security [2 hours]	**Webinar** IPv6 Associated Protocols Security [2 hours]	**Webinar** IPv6 Security Myths, Filtering and Tips [2 hours]
2.1.1 Identify the IPv6 security related fields of the IPv6 basic header	Module 2.1	Yes	Yes		
2.1.2 Identify the IPv6 security threats related to the IPv6 basic header	Module 2.1	Yes	Yes		
2.1.3 Identify the IPv6 security aspects of the IPv6 extension headers	Module 2.2	Yes	Yes		
2.1.4 Identify the IPv6 security threats related to IPv6 extension headers	Module 2.2	Yes	Yes		
2.1.5 Identify the IPv6 security aspects of the IPv6 addressing architecture	Module 2.4	Yes	Yes		
2.1.6 Identify the IPv6 security threats related to the IPv6 addressing architecture	Module 2.4	Yes	Yes		

Learning Resources

2.2 Security measures to protect from Basic IPv6 protocol security threats

	RIPE NCC Academy IPv6 Security [16 hours]	**Training Course** IPv6 Security [1 day]	**Webinar** Basic IPv6 Protocol Security [2 hours]	**Webinar** IPv6 Associated Protocols Security [2 hours]	**Webinar** IPv6 Security Myths, Filtering and Tips [2 hours]
2.2.1 Choose a suitable and available security measure for IPv6 security threats related to the IPv6 basic header	Module 2.1	Yes	Yes		
2.2.2 Choose a suitable and available security measure for IPv6 security threats related to the IPv6 extension headers	Module 2.2	Yes	Yes		
2.2.3 Choose a suitable and available security measure for IPv6 security threats related to the IPv6 addressing architecture	Module 2.3	Yes	Yes		
2.2.4 Identify the IPsec elements used by IPv6 to offer security in the IP layer	Module 2.3	Yes	Yes		
2.2.5 Choose the IPsec security protocol that offers the needed security	Module 2.3	Yes	Yes		
2.2.6 Choose the IPsec mode that best fits your security needs	Module 2.3	Yes	Yes		

Learning Resources

3. Security of Protocols Associated With IPv6

3.1 Security threats of protocols associated with IPv6

	RIPE NCC Academy IPv6 Security [16 hours]	**Training Course** IPv6 Security [1 day]	**Webinar** Basic IPv6 Protocol Security [2 hours]	**Webinar** IPv6 Associated Protocols Security [2 hours]	**Webinar** IPv6 Security Myths, Filtering and Tips [2 hours]
3.1.1 Identify the IPv6 security aspects of ICMPv6	Module 3.1	Yes		Yes	
3.1.2 Identify the IPv6 security threats related to ICMPv6	Module 3.1	Yes		Yes	
3.1.3 Identify the IPv6 security aspects of NDP	Module 3.2	Yes		Yes	
3.1.4 Identify the IPv6 security threats related to NDP	Module 3.2	Yes		Yes	
3.1.5 Identify the IPv6 security aspects of MLD	Module 3.3	Yes		Yes	
3.1.6 Identify the IPv6 security threats related to MLD	Module 3.3	Yes		Yes	
3.1.7 Identify the IPv6 security aspects of DNS	Module 3.4	Yes			
3.1.8 Identify the IPv6 security threats related to DNS	Module 3.4	Yes			
3.1.9 Identify the IPv6 security aspects of DHCPv6	Module 3.5	Yes			
3.1.10 Identify the IPv6 security threats related to DHCPv6	Module 3.5	Yes			

Learning Resources

3.2 Security measures to protect from IPv6 associated protocol security threats

	RIPE NCC Academy IPv6 Security [16 hours]	**Training Course** IPv6 Security [1 day]	**Webinar** Basic IPv6 Protocol Security [2 hours]	**Webinar** IPv6 Associated Protocols Security [2 hours]	**Webinar** IPv6 Security Myths, Filtering and Tips [2 hours]
3.2.1 Choose a suitable and available security measure for IPv6 security issues related with ICMPv6	Module 3.1	Yes		Yes	
3.2.2 Choose a suitable and available security measure for IPv6 security issues related with NDP	Module 3.2	Yes		Yes	
3.2.3 Choose a suitable and available security measure for IPv6 security issues related with MLD	Module 3.3	Yes		Yes	
3.2.4 Choose a suitable and available security measure for IPv6 security issues related with DNS	Module 3.4	Yes			
3.2.5 Choose a suitable and available security measure for IPv6 security issues related with DHCPv6	Module 3.5	Yes			

Learning Resources

4. Internet-Wide IPv6 Security

4.1 Internet-wide IPv6 security threats

	RIPE NCC Academy IPv6 Security [16 hours]	Training Course IPv6 Security [1 day]	Webinar Basic IPv6 Protocol Security [2 hours]	Webinar IPv6 Associated Protocols Security [2 hours]	Webinar IPv6 Security Myths, Filtering and Tips [2 hours]
4.1.1 Identify how Internet-wide IPv6 security threats could result in a DDoS attack or BGP hijack	Module 4.2	DDoS yes / BGP hijack as reference slides			
4.1.2 Match IPv6 security threats with the correct category of IPv6 Transition Mechanism	Module 4.3	Yes			

4.2 Security measures to protect from Internet-wide IPv6 security threats

4.2.1 Identify security measures to protect from IPv6 BGP Hijacking	Module 4.4	As reference slides			
4.2.2 Describe MANRS Actions that have an impact on IPv6 network security	Module 4.4	As reference slides			
4.2.3 Write basic rules and recommendations about IPv6 BGP Bogon Prefix Filtering	Module 4.4	As reference slides			
4.2.4 Match security measures with the correct threat and associated category of IPv6 Transition Mechanism	Module 4.3	Yes			

4.3 Filtering rules for IPv6 packets

4.3.1 Differentiate between two types of IPv6 filtering: packet forwarding vs. routing information	Module 4.1	Partially			
4.3.2 Choose filtering rules and recommendations for IPv6 packet filtering in order to improve the security of an IPv6 network	Module 4.1	Yes			Yes

Learning Resources

4.4 Available security options for IPv6 routing protocols

	RIPE NCC Academy IPv6 Security [16 hours]	**Training Course** IPv6 Security [1 day]	**Webinar** Basic IPv6 Protocol Security [2 hours]	**Webinar** IPv6 Associated Protocols Security [2 hours]	**Webinar** IPv6 Security Myths, Filtering and Tips [2 hours]
4.4.1 Choose the security options defined in the RIPng protocol standard	Module3.6	As reference slides			
4.4.2 Choose the security options defined in the OSPFv3 standard	Module 3.6	As reference slides			
4.4.3 Choose the security options defined in the IS-IS standard	Module 3.6	As reference slides			
4.4.4 Choose the security options defined in the MBGP standard	Module 3.6	As reference slides			

Support

If you have any questions regarding the exam, please send an email to Exams Support

Schedule Your Exam

To schedule your exam, please visit: https://exams.ripe.net/