3.5 IPv6 Forum Certified Security Course, Engineer, Trainer & Certification (GOLD)

The IPv6 Forum Certified Security Program (Security Course, Security Engineer, Security Trainer and Security Degree Exams Certification) expands the IPv6 Forum Gold certification programs in an area of very high importance to the IPv6 deployment and IPv6 operation teams as security is one of the most often cited concerns with the IPv6 enablement. IPv6 transition also presents a unique opportunity for IT organisations to implement comprehensive security architecture from day one.

The program defines and enforces a high standard for education and skills accreditation in the IPv6 Security specialty.

The program standardises:

- The requirements for an IPv6 Security course to be deemed complete and competitive in providing the requisite information
- The requirements for a Trainer to be deemed ready to deliver an IPv6 Security class effectively and with the necessary practical competency
- The requirements for an Engineer to demonstrate the level of expertise and competency necessary to be an effective IPv6 Security specialist.
- The requirements for an expert level industry certification to obtain IPv6 Security certified (Degree exams) certification status.

The standards defined by this program are enforced through the process of certification of IPv6 Security course content, of IPv6 Security trainers, IPv6 Security exams certification and of IPv6 Security engineers.

3.5.1 Requirements for the Gold IPv6 Security Course Content

To be eligible for the IPv6 Forum Gold “Security Course” certification, the content of the IPv6 security course must be reviewed against the requirements listed in this section. The review is conducted by IPv6 subject matter experts identified by the IPv6 Forum.

3.5.1.1 Course objectives

The IPv6 Security Course provides the students with the knowledge needed to understand the IPv6-specific aspects of IT security, the security implications of enabling IPv6 in the environment and the operational aspects of managing, from a security perspective, an IT environment during the transition to IPv6. It is important for the course to not limit the content to network security but cover multiple aspects of securing an IPv6 enabled IT environment. The course will provide the current best practices in implementing and operating a complete IPv6 security lifecycle.

3.5.1.2 Course audience and recommended prerequisites

This course is targeted to IT security architects, design and operations engineers, IT infrastructure architects, design and operations engineers, IT professional services engineers, application developers and security compliance and governance professionals who want to get an in-depth understanding of IPv6 security.

For an effective learning experience it is recommended that participants are familiar with IPv6 technology at least the level of IPv6 Forum Silver Engineer certification (or better). It is recommended that participants are familiar with the fundamental concepts of IT security.

3.5.1.3 Knowledge acquired by the student when completing the course

IT security in general and IPv6 security in particular are vast topics. To meet the IPv6 Forum Gold certification requirements the IPv6 Security course must at a minimum ensure that the following knowledge is acquired by the students:

- Scope of IPv6 Security in IT environment (from network to applications and from processes to policies and governance)
- IPv6 protocol architecture specific elements that impact or benefit IT security
- Vulnerabilities that are IP version independent and their mitigation
- Vulnerabilities that are IPv6 specific and their mitigation
- Methods for performing IPv6 security assessment of an IT environment
- Current IPv6 security best practices
- Development and implementation of security policies
- Key IPv6 considerations for IT security products (security control, security data collection, security information and event management, vulnerability and patch management) and requirements with respect to industry standards such as IPv6 Ready Logo, USG/NIST and RIPE501.

The key concepts are covered in a vendor independent context to avoid vendor specific implementation or support constraints.

Hands on skills acquired by the student when completing the course: Along with the knowledge provided through coursework, the Gold level IPv6 Security Course must help the student develop the following minimum set of practical skills:

- Capturing malformed IPv6 packets and identifying various threat vectors
- Observe IPv6 based reconnaissance techniques and mitigate against them
- Defining and implementing best practice policies for ICMPv6
- Observe and mitigate ICMPv6 DDOS attacks

- Updating security control (ACLs, policies, etc) for IPv6 on various infrastructure equipment (switches, routers, appliances)
- Observe and mitigate first hop security threats (RA protection, ND protection, etc.)
- Implement control plane (routing protocol) protection mechanisms
- Observe and mitigate security threats introduced by transition mechanisms (6to4, Teredo, 6PE, 6VPE, DS-Lite, 6rd, etc.)
- IPv6 securing hosts
- Configure IPsec for IPv6

The key concepts are covered in a vendor independent context to avoid vendor specific implementation or support constraints. The student should get hands on experience with commonly used security/hacker IPv6 tools. Labs should cover both transition and steady state scenarios.

3.5.1.4 Checklist of topics that must be covered by the course to qualify for Gold certification

The following topics must be covered in the Gold IPv6 Security course. For each topic, the material must cover the risk analysis, risk mitigation and best practices:

- Myths and realities regarding IPv6 security
- Security implications of IPv6 addressing architecture
    - Address and prefix size allocations
    - Address scoping
    - Privacy and Temporary Addresses
    - Cryptographically Generated Addresses
    - Special and Reserved addresses
- Security implications of IPv6 packet format
    - Main header format
    - Extension headers
- IPv6 and lower layer security mechanisms
    - 802.1x
    - Layer 2 controls
- First Hop security for IPv6
    - Neighbor Discovery (Protect ND State machine, SeND)
    - Router Discovery (Protect ND State machine, RA-Guard)
    - MLD Snooping
- Securing IPv6 provisioning mechanisms
    - Stateless Address Autoconfiguration
    - DHCPv6 (Stateless, Statefull, PD)
- Securing DNS
- Securing IPv6 Routing Protocols
- Securing IPv6 transport over MPLS networks
- Securing multicast for IPv6
- Securing IPv6 Transition Mechanisms
- Security considerations for dual-sacked hosts

- Security considerations for a virtualized compute infrastructure supporting IPv6
- IPv6 security considerations for applications
- Overview of IPv6 support in security products (FW, IPS, etc)
- IPv6 security assessment considerations
- Defining IPv6 security policies
- Implementing and managing IPv6 security policies
- IPv6 security hardening of infrastructure
- IPv6 forensics

It is expected but not required that the Gold IPv6 Security courses will start with an IPv6 essentials refresher.

3.5.2. Requirements for the Gold IPv6 Security Course Trainer Certification

A candidate qualifies for the Gold IPv6 Security Course Trainer certification if he or she meets the following requirements:

- Holds the Gold IPv6 Engineer certification
- Holds the Gold IPv6 Trainer certification
- Holds the Gold IPv6 Security Engineer certification
- Has been trained and evaluated by an IPv6 Forum approved Gold Certified IPv6 Security Trainer
- Successfully delivered at least one Gold Certified IPv6 Security Course under the observation of a Gold Certified IPv6 Security Trainer

No other industry certification is equivalent to the Gold IPv6 Security Trainer certification and can be used to lieu of the IPv6 Security Trainer Certification Process.

3.5.3. Requirements for the Gold IPv6 Security Engineer Certification

A candidate qualifies for the IPv6 Forum Gold IPv6 Security certification if he or she holds an active Gold IPv6 Engineer certification and one of the following requirements:

- Successfully completes the IPv6 Forum Security certification exam administered by an IPv6 Forum authorised testing organisation. The passing score is 75% or higher.
- Obtains a certification which has been approved by the IPv6 Forum as Gold IPv6 Security Certified Certification.

3.5.4. Requirements for the Gold IPv6 Security Certified Certification

In order to be certified as a Gold IPv6 Security Certified Certification, the required exams must cover all topics listed in section 3.5.1.3 and section 3.5.1.4. The exam topics must be covered in both written and lab exam (if applicable).

3.5.5. Application Process

The following information is required to apply for IPv6 Forum Certified Security Program:

1. Primary contact information
2. Certification program name
3. Certification program objective
4. If applying for IPv6 Forum Certified Security Course (Gold) list the topics covered in section 3.5.1.4.
5. If applying for IPv6 Forum Certified Security Engineer (Gold) see the requirements section 3.5.3 and provide supporting details.
6. If applying for IPv6 Forum Certified Security Trainer (Gold) see the requirements section 3.5.2 and provide supporting details.
7. If applying for IPv6 Forum IPv6 Security Certified Certification (Gold) see the requirements in section 3.5.4 and provide supporting details.