Training: F5
Securing NGINX Deployments

TRAINING GOALS:

Students will identify and administer client-side and upstream encryption (TLS) by specifying ciphers, Diffie-Hellman parameters, Perfect Forward Secrecy. Explore how to configure access control using limit rates and deny/allow lists and use dynamic SSL certificate loading. Introduce tips and best practices for securing NGINX like configuring HTTP/2 and HTTP/3 protocols. Become familiar with using the API Gateway and Secure API traffic using JWT authentication.

Audience

This course is for NGINX Administrators and Security Operations engineers who want an in-depth understanding of hardening NGINX security features.

CONSPECT:

- Chapter 1: Introduction
  - Define application security
  - Get familiar with the lab environment
  - Get started with a web application
- Chapter 2: Setting Up HTTPS
  - Secure web traffic
  - Learn basics of encryption using TLS
  - Configure an HTTPS NGINX server
- Chapter 3: Access Control
  - Set limits based on access, connections, and request rate
  - Set up audit, log and debug client connections
  - Use NGINX Plus key-value store
  - Describe methods for how TLS certificates are loaded in NGINX: traditional, dynamic lazy and dynamic in-memory
- Chapter 4: Authentication
  - Basic authentication
  - Sub request

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

    - Secure Links to content
- Chapter 5: Security Tips
    - Unprivileged (non-root) installation of NGINX Plus
    - HTTP versions
    - Traffic mirroring
- Chapter 6: Secure API Traffic
    - Understand the basics of NGINX API Gateway
    - Create a JWT Authentication Zone
    - Authenticate and sign API requests
- Chapter 7: Performance Tips and Resources
    - Tune TLS Handshake Operations (keepalive and Session Tickets)
    - Additional Resources

REQUIREMENTS:

Before taking this course, make sure you have completed one of the following:

- Administering NGINX for Web Services

The course assumes a basic understanding of networking, web servers, HTTP, load balancing, caching, proxying, and related concepts. Hands on labs are performed in a Linux environment. You will need to be able to navigate the file system from the command line and edit configuration files using VI/VIM. Additional experience with Linux environments will be helpful.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by F5 (course completion).

This course helps prepare participants for the F5 Certified Administrator, NGINX (F5-CA, NGINX) certification. The certification requires candidates to pass four exams: NGINX Management (F5CAN1); NGINX Configuration: Knowledge (F5CAN2); NGINX Configuration: Demonstrate (F5CAN3); and NGINX Troubleshoot (F5CAN4).

More information: https://education.f5.com/learning-path/view/24

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

TRAINER:

Certified F5 Networks Trainer

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310