



Enterprise Computing Solutions - Education Services

## NABÍDKA ŠKOLENÍ

---

**Prosím kontaktujte nás zde**

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: [training.ecs.cz@arrow.com](mailto:training.ecs.cz@arrow.com)

Phone: +420 597 488 811

# SOPHOS Sophos Firewall Certified Architect

<b>Kód:</b>	<b>DÉLKA:</b>	<b>CENA:</b>
SOP_FCEACH	24 Hours (3 DENNÍ)	Kč bez DPH 45,300.00

## Description

Školení je vedeno virtuálně v anglickém jazyce.

Cena školení je 1 500 GBP bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

The course is intended to be delivered in a classroom setting and consists of presentations and practical lab exercises to reinforce the taught content. Copies of the supporting documents for the course will be provided to each trainee.

Due to the nature of delivery, and the varying experiences of the trainees, open discussion is encouraged during the training.

The course is expected to take 3 days (24 hours) to complete, of which approximately 8 hours will be spent on the practical exercises.

## Cíle

On completion of this course, trainees will be able to:

Deploy Sophos Firewall in complex network environments

Explain how Sophos Firewall processes traffic and use this information to inform the configuration

Configure advanced networking and protection features

Protect web applications using the web server protection

Size hardware, virtual and software Sophos Firewalls for a given set of requirements

## Určeno pro

This course provides an in-depth study of Sophos Firewall, designed for experienced technical professionals who will be planning, installing, configuring and supporting deployments in production environments.

## Vstupní znalosti

Prior to taking this training, you should:

Have completed and passed the Sophos Firewall Certified Engineer course and any subsequent delta modules up to version 18.5

We recommend students have the following knowledge and experience:

Experience with Windows networking and the ability to troubleshoot issues

A good understanding of IT security

Experience configuring network security devices

Experience configuring and administering Linux/UNIX systems

If you are uncertain whether you meet the necessary prerequisites to take this course, please email us at [globaltraining@sophos.com](mailto:globaltraining@sophos.com) and we will be happy to help.

## Program

Recall important information from the Engineer course

Describe the deployment modes supported by the Sophos Firewall

Understand a range of scenarios where each deployment mode would commonly be used

Use built-in tools to troubleshoot issues

Labs (5 mins)

Module 1: Deployment (70 mins) Register for a Sophos Central evaluation

- Explain how the Sophos firewall can be accessed
- Understand the types of interfaces that can be created
- Understand the benefits of Fast Path technology
- Configure routing per firewall rule
- Understand best practice for ordering firewall rules
- Explain what Local NAT policy is and know how to configure it
- Labs (120 mins)
- Activate the Sophos Firewalls
- Post-installation configuration
- Bridge interfaces
- Create a NAT rule to load-balance access to servers
- Create a local NAT policy
- Configure routing using multiple WAN links
- Configure policy-based routing for an MPLS Scenario

Module 2: Base Firewall (120 mins) Install Sophos Central

- Explain what IPS is and how traffic can be offloaded to FastPath
- Demonstrate how to optimize workload by configuring IPS policies
- Examine advanced Intrusion Prevention and optimize policies
- Configure advanced DoS Protection rules
- Demonstrate how the strict policy can be used to protect networks
- Labs (15 mins)

Module 3: Network Protection (45 mins) Create advanced DoS Rules

Module 4: Synchronized Security (45 mins)

- Explain how Security Heartbeat works
- Configure Synchronized Security
- Deploy Synchronized Security in discover and inline modes
- Understand the advantages and disadvantages of deploying Synchronized Security in different scenarios
- Labs (40 mins)
- Configure source-based Security Heartbeat firewall rules
- Destination-based Security Heartbeat
- Missing Security Heartbeat
- Lateral Movement Protection

Module 5: Web Server Protection (60 mins)

- Explain how Web Server Protection works
- Describe the protection features
- Configure protection policies for a web application
- Configure web server authentication
- Publish a web service using the Web Application Firewall
- Use the preconfigured templates to configure Web Server Protection for common purposes
- Configure SlowHTTP protection
- Labs (90 mins)
- Web Application Firewall
- Load balancing with Web Server Protection
- Web Server Authentication and path-specific routing
  - Configure and deploy site-to-site VPNs in a wide range of environments
  - Implement IPsec NATing and failover
  - Check and modify route precedence
  - Create RED tunnels between Sophos Firewalls
  - Understand when to use RED
  - Labs (90 mins)
  - Create an IPsec site-to-site VPN
  - Configure VPN network NATing
  - Configure VPN failover
  - Enable RED on the Sophos Firewall
  - Create a RED tunnel between two Sophos Firewalls
  - Configure routing for the RED tunnel

Module 6: Site-to-Site Connections (90 mins) Configure route-based VPN

- Demonstrate how to configure and use RADIUS accounting
- Deploy STAS in large and complex environments
- Configure SATC and STAS together
- Configure Secure LDAP and identify the different secure connections available
- Labs (30 mins)
- Configure an Active Directory authentication server
- Configure single sign-on using STAS

Module 7: Authentication (40 mins) Authenticate users over a Site-to-Site VPN

Choose the most appropriate type for web protection in different deployment scenarios  
Enable web filtering using the DPI engine or legacy web proxy  
Configure TLS inspection using the DPI engine or legacy web proxy  
Labs (25 mins)  
Install the SSL CA certificate  
Configure TLS inspection rules

Module 8: Web Protection (50 mins) Create a custom web policy for users

Module 9: Wireless (45 mins)

Explain how Sophos Access Points are deployed and identify some common issues that may be encountered

Configure RADIUS authentication

Configure a mesh network

Configure Sophos Connect and manage the configuration using Sophos Connect Admin

Configure an IPsec remote access VPN

Configure an L2TP remote access VPN for mobile devices

Labs (30 mins)

Module 10: Remote Access (20 mins) Sophos Connect

Module 11: High Availability (60 mins)

Explain what HA is and how it operates

Demonstrate how to configure HA and explain the difference between quick and manual configuration

List the prerequisites for high availability

Perform troubleshooting steps and check the logs to ensure that HA is set up correctly

Explain the packet flow in high availability

Demonstrate how to disable HA

Labs (20 mins)

Create an Active-Passive cluster

Disable High Availability

Explain how Sophos Firewall fits into public cloud security architect

Deploy a Sophos Firewall on Azure and AWS

Configure Sophos Firewall for hybrid deployments

Deploy a high availability pair of Sophos Firewalls on Azure and AWS

Labs (45 mins)

Put a service in debug mode to gather logs

Retrieving log files

Troubleshoot an issue from an imported configuration file

Deploy a Sophos Firewall on Azure (Simulation)

Module 12: Public Cloud (45 mins) Deploy a Sophos Firewall on AWS (Simulation)

## Zkoušky a certifikace

To become a Sophos Certified Architect, trainees must take and pass an online assessment. The assessment tests their knowledge of both the presented and practical content. The pass mark for the assessment is 80% and is limited to 3 attempts.

## Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

## Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)