

# Fundamental of Cisco Firewall Threat Defense & Intrus. Prev.

Kód kurzu: SFWIPF

Cílem kurzu je ukázat, jak používat a instalovat Cisco Firepower Threat Defense platformu. Kurz naučí zájemce projít počáteční instalaci Firepower včetně směrování, vysoké dostupnosti, migrace z Cisco ASA platformy, řízení provozu a pravidel NAT. Dále účastník získá znalosti implementace "next-gen" vlastností, jako je IPS, Secure Intelligence, detekce přenášených souborů a ochrana před malware, který může být přenášen na síti. Účastník získá i zkušenosti s implementací VPN (Site-To-Site, Remote-Access), SSL dešifrování a základní administraci spojenou s řešením problémů na zařízeních.

Pobočka	Dnů	Cena kurzu	ITB
Praha	5	89 900 Kč	0
Brno	5	89 900 Kč	0
Bratislava	5	2 690 €	0

Uvedené ceny jsou bez DPH.

## Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita
11.05.2026	5	89 900 Kč	Online	EN	ALEF NULA - Online
18.05.2026	5	89 900 Kč	Prezenční	CZ/SK	ALEF NULA
21.09.2026	5	89 900 Kč	Prezenční	CZ/SK	ALEF NULA
12.10.2026	5	2 690 €	Online	CZ/SK	Online
12.10.2026	5	2 690 €	Prezenční	CZ/SK	Bratislava

Uvedené ceny jsou bez DPH.

## Požadované vstupní znalosti

Znalost TCP/IP protokolu, Základní znalosti směrování, Znalost principu Firewall, VPN a IPS.

## Studijní materiály

Účastníci obdrží přístup k elektronické verzi studijních materiálů.

## Lektor

Školitelé mají zkušenosti z praxe a jejich odbornost je potvrzena řadou mezinárodních certifikací nejvyšších úrovní. V případě specifických znalostí spolupracujeme s externími lektory a odborníky, s těmi nejlepšími v dané problematice.

## Osнова kurzu

- Obecný popis platformy Cisco FTD
- Základní instalační kroky FTD
- Implementace NGFW traffic control
- Implementace NAT
- Konfigurace Network Discovery
- Implementace Access Control Policy
- Implementace Security Intelligence
- Popis fungování detekce přenesených souborů a analýzy malware
- Popis a konfigurace next-generation IPS
- Konfigurace a řešení problémů spojených s site-to-site VPN
- Implementace remote VPN
- konfigurace SSL politik

### GOPAS Praha

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved

# Fundamental of Cisco Firewall Threat Defense & Intrus. Prev.

- Analýza událostí v centrálním management Firepower Management Centru
- Administrace Firepower Management Centra
- Řešení běžných problémů

#### **GOPAS Praha**

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

#### **GOPAS Brno**

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

#### **GOPAS Bratislava**

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved