FORTINET®
Training Institute

Fast Track Reference Guide

Network Security

Workshop Title	Short Name	Solution Area	Products	Objectives
Deploying Security Strategies for the Modern Network	Network Security	Secure Networking	• FortiGate • FortiSwitch • FortiAnalyzer • FortiManager • FortiSandbox • FortiClient EMS • FortiAuthenticator • FortiProxy	• Configure basic FortiGate settings for routing, firewall policies, and security profiles • Setup a Fortinet Security Fabric with centralized logging, visibility, and automation • Segment and secure the network with ISFW, ZTNA, and ADVPN for optimized remote access and WAN usage • Set up a FortiProxy secure web gateway with web access authentication, perform image analysis, and view log output
Constructing a Secure SD-WAN Architecture	SD-WAN	Unified SASE	• FortiGate • FortiManager	• Configuring SD-WAN via FortiManager • Setting up IPsec VPN • Installing the managed gateway policies • Configure VPN tunnel endpoints • Creating an SD-WAN template • Cloning a template • Assign and install the template • Edit the default route • Examining the configurations • Verify the failover to VPN • Verify return to MPLS
LAN Edge Wired and Wireless Max Students: 32 Instructors: Check the calendar for availability	SD-Branch	Secure Networking	• FortiGate • FortiSwitch • FortiAP • FortiManager	• Create a FortiLink interface • Authorize FortiSwitch and FortiAP • Create VLANs and policies • Create SSIDs • Configure radio frequency (RF) • Assign firewall policies to FortiGate • Manage FortiSwitch and FortiAP with FortiManager

Network Security

Workshop Title	Short Name	Solution Area	Products	Objectives
What's New in FortiOS	FortiOS	Secure Networking	• FortiAnalyzer • FortiGate • FortiManager • FortiSwitch • FortiClient EMS • FortiClient	• GUI updates: packet capture and debug flow, user interface themes, dynamic routing • Security-driven networking: SD-WAN orchestration, API preview • AI-Driven security operations: improved automation workflow • Next generation firewall: workflow management, web filtering • Secure access switching: FortiSwitch management • Configure FortiClient EMS and FortiGate ZTNA Application Gateway for secure remote access to applications • Security Fabric: Fabric management page, FortiAnalyzer reports, Security Fabric in multi-VDOM mode

Cloud Security

Workshop Title	Short Name	Solution Area	Products	Objectives
Advanced Email Security Solution	Email Security	AI-driven Security Operations	• FortiMail • FortiIsolator	• Session profiles • Antivirus/Antimalware • Impersonation Analysis • Content Disarm and Reconstruction • URL Click Protection • Identity-based Encryption
Application Delivery Without Limits	ADC	Unified SASE	• FortiADC	• Simplify scalability of web applications within the data center • Provide global redundancy for web applications • Improve performance of web applications using SSL offloading • Protect and secure web applications with built-in firewall, WAF, and more
Web Applications and API Security	Web Security	Unified SASE	• FortiGate	• Perform initial vulnerability testing • Create a protection profile • Configure and secure local logging • Remote logging with FortiAnalyzer • Secure resource access using authentication and page enforcement • Implement certificates and encryption • Protect against zero-day attacks using machine learning • Perform an injection attack and use FortiWeb to protect against it • Secure your cookies with FortiWeb

Cloud Security

Workshop Title	Short Name	Solution Area	Products	Objectives
Security, Visibility, and Control of Public Cloud Infrastructure and Workloads	Public Cloud	Unified SASE	• FortiGate • FortiWeb • FortiSandbox • FortiAnalyzer	• Use Terraform to programmatically provision resources and Fortinet appliances • Extend the Security Fabric to cloud based resources • Use Fabric connectors to define security policies based on asset labels/tags • Visualize cloud-based activity using FortiView on FortiGate • Dynamically modify FortiGate configurations with Terraform
Defend and Protect Against Disruptions to Your Infrastructure	DDOS	Secure Networking	• FortiDDoS • FortiGate	• Setup and configure FortiDDoS from scratch • Configure Service Protection Profiles and protection sub-nets • Generate and characterize an attack • Reduce false positive DDoS attacks • Differentiate between FortiDDoS and statefull firewalls

Security Fabric

Workshop Title	Short Name	Solution Area	Products	Objectives
Reduce the Complexity of Operations with Centralized Management	Fabric Management	AI-driven Security Operations	• FortiManager • FortiGate	• Understand the benefits of using the Fabric Management Center • Reduce operational complexity and security risk by simplifying and automating deployment and network monitoring • Centrally manage a device's configuration, including policies, IPsec VPN, and SD-WAN, using the GUI and scripts • Improve time to compliance readiness with pre-built reports, as well as customize and create new reports • Reduce risk by automating response to security events with network-aware response actions
Streamlining Automation Using Web Services APIs	API	Unified SASE	• FortiManager • FortiGate	• Benefit from leveraging Fortinet's JSON & RESTful API's. • Use Fortinet's native automation tools via Webhooks to interact with other security vendors. • Interact with FortiManager and FortiGate API endpoints using Python, DevOps Automation and Fortinet Developer Network (FNDN).
Creating a Comprehensive Fortinet Security Fabric	Security Fabric	Secure Networking	• FortiGate • FortiManager • FortiAnalyzer • FortiSandbox • FortiWeb	Configure a Security Fabric to integrate: • Multiple FortiGate devices • FortiManager/FortiAnalyzer • FortiSandbox • FortiWeb

Security Analytics

Workshop Title	Short Name	Solution Area	Products	Objectives
Breaking the Kill Chain with AI-Driven Breach Protection	Breach Protection	AI-driven Security Operations	• FortiGate • FortiClient • FortiSandbox • FortiMail • FortiNDR • FortiDeceptor • FortiManager	• Apply solutions in different stages of the kill chain • How to detect advanced and zero-day threats • How to disrupt threat actors • How to bolster security operations • includes challenge to protect an organization from attack
Powerful Security Information and Event Management	SIEM	AI-driven Security Operations	• FortiSIEM • FortiGate	• Understand CMDB and FortiSIEM architecture • Use FortiSIEM features • Run analytic searches • Investigate UEBA events • Use rapid detection and remediation of security events • Use security and performance management
Simplify SOC with Security Fabric Analytics and Automation	Analytics	AI-driven Security Operations	• FortiAnalyzer • FortiGate	• Understand the benefits of using FortiAnalyzer to simplify SOC operations • Use playbooks to automate workflows and reduce the workload on the security team • Use FortiGate event handlers to automate actions via automation stitches • Work with analytics logs and generate custom reports

Security Analytics

Workshop Title	Short Name	Solution Area	Products	Objectives
Empowering Security Operations Leveraging SOAR	SOAR	AI-driven Security Operations	• FortiSOAR • FortiGate	• Automating routine tasks to preserve scarce expertise for critical incidents • Use connectors that integrate with deployed security controls to ingest information and provide a single, centralized point of visibility and control • Aggregate security alerts in one place, enriched with added context to speed investigation, and including playbooks to guide the triage process
Performance and Security Testing	Tester	AI-driven Security Operations	• FortiTester • FortiGate • FortiWeb	• Perform Malware Security Testing against FortiGate. • Perform IPS Security Testing against FortiGate. • Perform DDOS Security Testing against FortiGate. • Perform Web protection testing against FortiWeb. • Implement MITRE ATT&CK using FortiTester.

Edge Security

Workshop Title	Short Name	Solution Area	Products	Objectives
Proactive Advanced Endpoint Detection and Response	Endpoint	Unified SASE	• FortiEDR • FortiGate	• Overview of FortiEDR Central Manager and components • Deploy FortiEDR collector • Configure FortiEDR pre & post-execution security policies • Investigate, filter, sort, and view threat events in FortiEDR • Perform forensic analysis in FortiEDR • Generate Security Reports and create Exceptions
Securely Embrace the IoT Revolution with NAC	NAC	Secure Networking	• FortiNAC • FortiGate • FortiSwitch	• Achieve network and endpoint enhanced visibility • Configure dynamic control capabilities • Create automated responses for rapid threat mitigation • FortiGate VPN device Integration
Securing the Hybrid Workforce with SASE	SASE	Unified SASE	• FortiSASE	• Achieve Secure Internet Access (SIA) and Secure SaaS Access (SSA) for any user using FortiSASE • Setup Secure Private Access (SPA) to internal resources using FortiSASE • Use FortiSASE Universal ZTNA • View FortiSASE Logs and Reports NOTE: Due to demo infrastructure limitations, participants will be provided with a read-only lab environment. While attendees will be able to navigate and review the user interface, no configuration changes will be possible.

Edge Security

Workshop Title	Short Name	Solution Area	Products	Objectives
The Evolution of Access to Applications with Fortinet ZTNA	ZTNA	Unified SASE	• FortiGate • FortiClient EMS • FortiClient • FortiPAM • FortiAuthenticator	• Configure FortiClient Endpoint Management Server (EMS) to extend comprehensive protection to remote users • Scan Vulnerabilities and further patch them to strengthen the organization's security measures using FortiClient Endpoint Protection Platform (EPP) • Configure ZTNA HTTPS Application Gateway for secure remote access to applications • Set up Dial-Up VPN connections and demonstrate secure access to internal resources • Implement SAML for enhanced security during accessing resources • Deploy Zero Trust Network Access (ZTNA) by configuring tags, ZTNA server, rules, and full-mode ZTNA policy for context-based posture checks, ensuring secure application access • Configure FortiPAM proxy rules and ZTNA to augment security measures • Showcase user access to FortiGate (FGT) through FortiPAM • Set up folder and secret access for administrators and IT contract users to manage permissions effectively. • Demonstrate the seamless operation of these critical functions, ensuring participants can effectively secure remote access environments

Challenge

Workshop Title	Short Name	Solution Area	Products	Objectives
Attack and Defense Methodologies	Attack & Defend	Secure Networking	• FortiGate • FortiMail • FortiWeb • FortiClient • FortiSandbox • FortiManager • FortiAnalyzer	Team Challenge where participants compete against each other in teams for the best score. Includes Leaderboard for real-time display of team scores. • Includes two independent challenges which can be delivered as a single event, or individually: • Attack Challenge: Using threat actor's tools and techniques to breach an organization and retrieve sensitive information from a fictitious organization • Defend Challenge: Using FortiGate, FortiMail, FortiWeb, FortiSandbox, and FortiClient-EMS to break the kill chain
Threat Hunting using MITRE ATT&CK™ TTPs to Identify Adversarial Behaviors	Threat Hunting	AI-driven Security Operations	• FortiGate • FortiEDR • FortiSOAR • FortiDeceptor • FortiSandbox • FortiAnalyzer • FortiMail • FortiWeb	• Educational challenge where participants will assume the role of a security analyst and be asked to identify any undetected threats on AcmeCorp's network. • To do this participants will make use of Mitre ATT&CK™, which is a knowledge base of adversarial behavior based on real-world observations. • ATT&CK™ allows analysts to hunt for patterns of behavior rather than artifacts such as hashes, IPs, or Domains. Why is this important? Well, according to 'The Pyramid of Pain' by David Bianco, while it is very easy for attackers to change these artifacts it is much harder for them to change their Tactics, Techniques, and Procedures (TTPs). Therefore, TTPs are a more reliable way of identifying adversary behavior. • The challenge is set up with several exercises set around the technical goals the adversary is trying to achieve (ATT&CK™ Tactics), for example, Initial Access, Persistence, Privilege Escalation, Command and Control. You will be asked to detect any techniques being used by an adversary to achieve these goals.

Industry Verticals

Workshop Title	Short Name	Solution Area	Products	Objectives
Cybersecurity for Safe, Reliable, Secure Industrial Control Systems (ICS)	OT	Industry Verticals	• FortiGate • FortiNAC • FortiSwitch • FortiDeceptor • FortiTester	• OT business drivers and security priorities • Differences between IT and OT • The importance of actively securing OT environments • Leveraging the Purdue Model • Applying the Security Fabric to secure OT • Expanding the Security Fabric and enhancing the value of Fabric-ready partners
Digital Security Engineered for Digital-Age Education	Education	Industry Verticals	• FortiGate • FortiClient EMS • FortiClient • FortiEDR • FortiManager	• Configure and leverage NGFW capabilities of FortiGate in your environment. • Configure FortiClient EMS and FortiGate ZTNA Application Gateway for secure remote access to applications • FortiEDR can provide endpoint protection and help analyze and classify potentially malicious events • Use SD-WAN Templates to facilitate SD-WAN deployments via FortiManager.
Solving the Financial Services Cybersecurity Challenge	Finance	Industry Verticals	• FortiGate • FortiClient EMS • FortiClient • FortiWeb • FortiAuthenticator • FortiManager	• Setup FortiGate and EMS security fabric integration. • Configure ZTNA remote worker & on-net. • Perform FortiWeb basic setup. • Perform Credential stuffing defense. • Protect against Injection attacks. • Configure FortiAuthenticator Fortinet Single-Sign-On. • Configure FGT admin access with 2FA using FortiAuthenticator. • Setup Secure SD-WAN connection between HQ and Branches.

Industry Verticals

Workshop Title	Short Name	Solution Area	Products	Objectives
Network Security Solutions for the Healthcare Industry	Healthcare	Industry Verticals	• FortiGate • FortiClient EMS • FortiClient • FortiEDR • FortiManager	• Configure and leverage NGFW capabilities of FortiGate in your environment. • Configure FortiClient EMS and FortiGate ZTNA Application Gateway for secure remote and local access to applications • FortiEDR can provide endpoint protection and help analyze and classify potentially malicious events while provding virtual software patching • Use SD-WAN Templates to facilitate SD-WAN deployments via FortiManager using Meta variables.
Protecting the Always-On Retail Customer Experience	Retail	Industry Verticals	• FortiGate • FortiAnalyzer • FortiManager • FortiMail	• Configure and manage the Fortinet Security Fabric • Configure SD-WAN between multiple sites • Prevent business email compromise (BEC) attacks


FORTINET