Both Microsoft Azure and Fortinet’s Azure program are growing at a near-record pace. There has been broad interest from both Microsoft and Fortinet to share a deeper level of knowledge on our mutual solutions so that we can drive more business and a better customer experience. With that in mind this session will include a mixture of presentations, demonstrations and hands-on-lab style and approach to learning about both the Microsoft Azure Cloud Services and the Fortinet FortiGate Azure Integration. It will cover the core concepts of the Microsoft Azure Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), which gives you the knowledge to build, deploy and manage applications and services, such as the Fortinet FortiGate Azure Virtual Appliance through a global network of Microsoft Managed datacenters.

- Microsoft Cloud Overview
- IaaS, PaaS and SaaS approach from Microsoft
- Key examples of how enterprises are using these with highlights of enterprises who are using multiple implementations in production
- Security in Microsoft’s Cloud
- Core capabilities
- Shared responsibility model
- Windows Azure Network Services Overview
- Virtual networks | UDR
- Microsoft Azure Resource Manager Overview

**Technical Requirements:** Laptop with 8Gb RAM and Wifi. Modern web browser. SSH/Telnet terminal client.

**Skills Requirements:** NSE-4

**Duration:** 4 hours

**Products List:** FortiGate, Microsoft Azure
CLOUD SECURITY - AWS

Level: Advanced

Speakers List: Pravesh Lokesh


Skills Requirements: NSE-4

Duration: 4 hours

Amazon Web Services has made itself one of the leaders for Cloud hosting by providing not just virtual machines, but configurable services and software implementations of hardware found in data centers. For most large scale systems, the move to Cloud infrastructure brings to the table a huge set of questions on how to handle issues such as load balancing, networks, failover, and security. The AWS suite can handle the same issues that a physical data center can, usually for a fraction of the cost.

Using cloud computing instead of buying new infrastructure is becoming the new normal. In fact, for many organizations, it has become the default choice. Cloud computing fulfills rapid IT environment provisioning needs, allows use of on-demand applications, and enables companies to analyze big data as storage requirements grow. AWS Partner Network (APN) Advanced Technology Partner Fortinet delivers a cost-effective Security-as-a-Service (SaaS) solution on AWS that can help lower operational expenses and reduce security complexity, helping customers fulfill their duties of the AWS Shared Responsibility Model. Fortinet provides advanced threat protection to a variety of environments including data centers, environments with distributed locations, and branch offices. Security appliances from Fortinet seamlessly integrate with Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (Amazon VPC) to minimize risk and mitigate security threats for workloads running on the public cloud.

1. Introduction to Amazon Web Services Cloud Computing Platform and Infrastructure (AWS Regions, Route53, Terminology etc.)
2. Get hands on experience using the Amazon Web Services Computing Platform and Infrastructure
3. Deep Dive into the specific FortiGate AWS Features and Architecture (Common Deployment Models etc.)
4. FortiGate in AWS Design Considerations
5. AWS VPC Walkthrough
6. Challenges

- Amazon Elastic Load Balancer (ELB) Sandwich FortiGate Demonstration
- FortiGate HA Setup in a VPC and Cloud Formation Template Setup (Hands-on-Lab)

When going through this Hands-on-Lab, you will be following the steps laid out below:

- **Step 1)** Download the CloudFormation template
- **Step 2)** Login to AWS Management Console using your AWS login credentials
- **Step 3)** Navigate to CloudFormation service in the Management Tools Section of the Management Console
- **Step 4)** Create Stack
- **Step 5)** Upload the template to Amazon S3
- **Step 6)** Create a stack name to identify the CloudFormation stack
- **Step 7)** Choose the appropriate values for the parameters listed in the parameter section.
- **Step 8)** Click Next and provide a key name (optional)
- **Step 9)** Create the Stack
- **Step 10)** Wait for the CloudFormation service to finish creating all the resources
- **Step 11)** Once the stack is created, the Output section has the login information for the Firewall and the Worker Node
- **Step 12)** Login to the FortiGate firewall through ssh/https; configure the firewall with your required security features
- **Step 13)** Login to the Worker Node using ssh
- **Step 14)** Navigate to the folder fortigateha once you are logged into the worker node
- **Step 15)** Execute the python script fortigateha.py with the runtime variable stack name. python fortigateha.py

*Once this is done, FortiGate HA setup is complete.*

Products List: FortiGate, Amazon Web Services
FORTIAUTHENTICATOR AND CLOUD SINGLE-SIGN ON

Level: Advanced

Speakers List: Kash Valji


Skills Requirements: Previous hands on experience with a FortiAuthenticator deployment or workshop

Duration: 4 hours

Advanced FortiAuthenticator Workshop starting with RADIUS troubleshooting techniques (Tools, Debugging and Performance Testing).

Establishing an understanding of how SAML works and enables Web SSO.

Focusing on Cloud Single Sign-On, understanding how to integrate on-premise FortiGate with Cloud providers such as Office 365 and Google G Suite.

Hands-on configuration of FSSO between an on-premise FortiGate and a 3rd Party Cloud Provider (Okta).

Looking at FortiAuthenticator Two-Factor Authentication with Cloud Providers such as Office 365.

(Time permitting: FortiAuthenticator and 802.1X Best Practice)

Products List: FortiGate, FortiAuthenticator, Windows Active Directory, Cloud SSO Solution (Okta)
FORTISIEM - ACHIEVING A SUCCESSFUL DEPLOYMENT

Level: Mix

Speakers List: Dan Hanman, Robert Pluim, Dušan Tomić, Michał Kułakowski


Skills Requirements: No previous FortiSIEM knowledge is required, good all round IT or security knowledge

Duration: 1 day

SIEM deployments are notoriously time consuming, difficult and pitted with failures. This full day workshop will walk you through the concepts SIEM solutions, how to keep things simple and achieving successful deployments. You get hands on skills using FortiSIEM through a structured workshop and by the end of the workshop you will be comfortable with:

- Discovering (adding) devices to be monitored
- Performing analytic searches and summarising events
- Creating Rules and using the Incident Interface
- Building Dashboards and Reports
- (Time permitting - overview of custom parsers (device support))

With these skills plus other topics on the course you will be well prepared to successfully deploy FortiSiEM and start getting the maximum value from the platform.

Products List: FortiSIEM
APPLICATION SECURITY FOR THE DATA CENTER

Level: Basic, Advanced, Mix

Speakers List: Rafael Lehmani, Rafael Gracioli, Roy Scotford, Raúl Barragán, Ferry Kemps


Skills Requirements: NSE-4 and/or NSE-6 - good understanding of the concepts of Web Application Firewall, Application Delivery Controllers (Global Load Balancing, Server Load Balancing), DDoS attacks and defenNSE-mechanisms. Experience with any of the products: FortiWeb, FortiDDoS and FortiADC. Basic FortiGate configuration.

Duration: 1 day

This session covers Fortinet's Integrated Application Security Solution: a complete end-to-end high-performance solution that protects an organization's valuable information throughout the data center. You will have an in-depth look and troubleshoot these components of the solution:

- FortiDDoS: DDoS Protection for the whole Data Center, including Layer 7 attack protection
- FortiWeb: Web Application Firewall for complete protection against known and zero-day attacks
- FortiADC: Secure Application Delivery with Availability, Scalability and Performance

You will also see how to expand the solution across multiple data centers to offer redundancy and improve performance.

Topics covered:

- Global Load Balancing
- Advanced L7 Server Load Balancing
- Scripting
- SSL offloading
- Web Application behavioral protection
- Multi-Vectors DDoS attack mitigation

Products List: FortiWeb, FortiDDos, FortiADC, FortiGate
HOW TO BUILD THE FORTINET ATP FRAMEWORK ATP A

Level: Beginners

Speakers List: Kash Valji, Khaled Hassan, Alain Forcioli


Skills Requirements: NSE-4

Duration: 4 hours

This proven and updated session is designed for beginners who want to embrace the ATP framework which is a key pillar of the Fortinet Security Fabric. The purpose is to build and to configure the Fortinet products which are required to protect efficiently a network from advanced or targeted attacks. In this session you will learn what are the components of the Fortinet ATP framework and how they interact each other for building a security fabric.

**CYBER RANGE**

**Level:** Advanced

**Speakers List:** Khaled Hassan, Alain Forcioli

**Technical Requirements:** Laptop with 8Go RAM (preferably 16GB) and Wifi. Modern web browser. SSH/Telnet terminal client.

**Skills Requirements:** NSE-4

**Duration:** 4 hours

Attendees will be involved in a cyber warfare training with the purpose of receiving a cybersecurity education. A real-world networked environment based on virtual machines acting as web and mail servers and other types of machines as well will be simulated. It will be the playground for a real-time competitions between multiple players.

Attendees will be required to advance through various operational scenarios through which they will understand offensive and defensive cyber security methods.

Attendees will gain the required knowledge allowing them to react upon on-going advanced/targeted attacks blended into a mix of malicious and non-malicious traffic.

**Products List:** FortiAnalyzer, FortiClient, FortiGate, FortiMail, FortiSandbox, FortiSwitch, FortiWeb.
HOW TO INTEGRATE WIRELESS SOLUTIONS (INTEGRATED, CLOUD AND CONTROLLER) TO THE SECURITY FABRIC

Level: Mix - Advanced

Speakers List: Vincent Ribiere, Flavien Richard, Brian Andersen, Eric Mouque

Technical Requirements: Laptop with 8Go RAM and Wifi. Modern web browser. SSH/Telnet terminal client. Delegate’s FGT-61E.

Skills Requirements: Wireless skills

Duration: 1 day

Wi-Fi is becoming the primary access medium for many of these network devices. Reliable Wi-Fi is critical infrastructure for all enterprises; connectivity, performance and security are all required. Wi-Fi usage continues to expand and shows no sign of slowing down:

- 6.5+ Million new Wi-Fi devices shipped every day
- 33+ Billion devices estimated to be connected by 2020
- Internet of Things (IoT) will just exacerbate these trends

A recent Gartner quote stated that as a result of this growth “80% of newly installed wireless networks will be obsolete because of a lack of proper planning.” Let’s see how the Fortinet Wireless solutions can address this needs.

This session will cover how to integrate FOS 5.6 Wireless controller into the Security fabric. You will also get an update on FortiAP Universal AP and how to use it. We will also discuss how to use FortiConnect and the Controller solution for Guest on boarding and user profiling.

Topics covered:
- How to design a reliable Wi-Fi infrastructure (design guidelines and Best practices)
- Guest on boarding using FortiConnect
- What are the benefits of FortiWLC 8.3.x and how to manage Wireless solution with FortiWLM
- How FOS 5.6 Wireless controller is now integrated in the Security Fabric
- How to enable Security fabric at the edge with FortiCloud
- Wireless products roadmap

Products List: FortiGate, FAP, FAC, Connect, FortiWLC, FortiWLM.
ENTERPRISE SECURE ACCESS WITH FORTISWITCH

Level: Mix

Speakers List: Rafael Gracioli, Raúl Barragán


Skills Requirements: NSE-4 and/or NSE-6 - good understanding of common switching technologies, device discovery and authentication methods (LLDP-MED, MAB, 802.1x), and basic configuration of FortiGate, FortiAuthenticator and FortiManager.

This session shows how to simplify deployment and operations of enterprise secure access scenario, with FortiSwitch as part of Fortinet Security Fabric. You will experience the FortiGate single pane of glass management to set up and provision the access network (FortiSwitch), then use device discovery and port security policies to control access to the network in an office environment.

FortiGate Switch Controller functionality (FortiLink) offers benefits such as zero-touch provisioning, secure configuration management, centralized provisioning and maintenance.

Topics covered:
- FortiGate switch controller (FortiLink) with MLAG for efficient network connectivity
- Port Security
- Dynamic VLAN assignment with 802.1x
- Device Discovery with LLDP-MED
- Bandwidth Management
- Centralized management with FortiManager

Products List: FortiSwitch, FortiGate, FortiManager, FortiAuthenticator, and FortiVoice/FortiFone
A DEEP DIVE INTO FORTIOS WITH THE SUPPORT TEAM

Level: Advanced

Speakers List: Laurent Blossier, Cédric Gustave, Stéphane Hamelin, Robin Hardy, Alex Vizzari


Skills Requirements: NSE-4 and/or NSE-7 - A good working knowledge of the FortiGate and FortiOS with the ability to use the GUI and CLI commands for troubleshooting purposes.

Duration: 4 hours

This session is split into 2 sub sessions with hands on labs. You will learn how to configure, optimize and troubleshoot the FortiGate in various deployment scenarios.

Topics covered:
- Understanding and troubleshooting FortiGate High Availability
- Fortinet FGCP clustering (A-P, virtual-cluster, A-A)
- Fortinet FGSP clustering
- HA and session sync
- HA and routing
- HA and IPsec
- FortiGate memory management
- Identifying issues
- Optimization

Products List: FortiGate
SECURITY OPERATION – ADVANCED SECURITY & ANALYTICS MANAGEMENT (FMG/FAZ 5.6)

Level: Beginner / Intermediate

Speakers List: Jean-Pierre Forcioli, Roland Stierli

Technical Requirements: Laptop with 8Go RAM (preferably 16GB) and Wifi. Modern web browser. SSH/Telnet terminal client.

Skills Requirements: NSE-4

Duration: 4 hours

This two parts session will showcase 1) two of the most important FortiManager features for the enterprise and the telco/MSSP customers: VPN Management and Automation with API, and 2) the latest and greatest improvements brought to FortiAnalyzer 5.4.x/5.6.x.

• FortiManager: VPN Management made easy: we will have a deep dive of the new VPN Manager module, from its new Monitoring view to its new flexible static routing options or custom zones usage. Automation made easy: we will present the power of the FortiManager JSON API and the FortiOS REST API. FortiManager Design made easy: will describe everything you need to know about Device & ADOM DB.

• FortiAnalyzer: Architecture, design and best practice for sizing- learn how to secure the log communication - Update on the most recently added security analytic and coloration capabilities (FortiView, NOC/SOC, IOC) - practical usage examples for their APIs and reference cases.

Products List: FortiManager, FortiAnalyzer, FortiGate
ENDPOINT SECURITY AS THE ULTIMATE LAYER FOR THE SECURITY FABRIC

Level: Beginner

Speakers List: Alain Forcioli

Technical Requirements: Laptop with 8Go RAM (preferably 16GB) and Wifi. Modern web browser. SSH/Telnet terminal client.

Skills Requirements: NSE-4

Duration: 4 hours

Through hands-on labs, the attendees will install and configure the Enterprise Management Server which is the Endpoint central Management solution for FortiClient endpoints. They will learn how to deploy and provision endpoints in a network. They will also discover the role and the value of the FortiClient endpoint when it comes to the Fortinet Security Fabric.

Products List: FortiAnalyzer, FortiClient, FortiClient EMS, FortiGate, FortiSandbox.
FORTIOS – ADVANCED FEATURES

Level: Advanced

Speakers List: Murat Kelesoglu, Sean Groarke, Alexei Parchkov, Roshanak Partovi, Emmanuel Lety

Technical Requirements: Laptop with 8Go RAM (preferably 16GB) and Wifi. Modern web browser. SSH/Telnet terminal client.

Skills Requirements: NSE-4

Duration: 4 hours

This session covers selected advanced features of FortiOS. A deep dive overview will be followed by use-cases, configuration and optimization tips. Hands-on labs will allow you to explore/put in practice the discussed topics.

Topics covered are Explicit proxy, Content filtering (SSL Deep Inspection), IPSec VPN and SSL VPN.

Products List: FortiGate
FORTIOS 5.6 AND SECURE FABRIC

Level: Advanced

Speakers List: Murat Kelesoglu, Sean Groarke, Alexei Parchkov, Roshanak Partovi, Emmanuel Lety

Technical Requirements: Laptop with 8Go RAM (preferably 16GB) and Wifi. Modern web browser. SSH/Telnet terminal client.

Skills Requirements: NSE-4+, good working knowledge of FortiOS

Duration: 4 hours

This session covers selected new features implemented in FortiOS 5.6. A deep dive overview will be followed by use-cases, configuration and optimization tips. Hands-on labs will allow you to explore/put in practice the discussed topics.

Topics covered are Cooperative Security Fabric, SD-WAN, Flow vs Proxy modes, Vxlan, NGFW policy mode and NAT mechanisms (overview + 5.6 new).

Products List: FortiGate
HANDLING FORTICLOUD SERVICES

Level: Mix

Speakers List: Emmanuel Rabatan


Skills Requirements: NSE-4

Duration: 4 hours

This session is designed to discover and test all available FortiCloud service. The market is moving to more externalized services and cloud applications because companies are more inclined to accept OPEX costs. SMB market is also interested by more affordable services and less hardware devices to maintain.

FortiCloud services have been designed to help partners and customers adopt new technologies and get higher security. FortiSandbox Cloud, FortiCloud Threat Detection, Forticloud AP for Smart AP offer a real competitive advantage. Partners may also be creative and propose offers based on FortiCloud services such as Forticloud Management, FortiPortal or FortiDeploy

ADVANCED SECURITY IN VMWARE SDDC WITH FORTIGATE-VMX

Level: Mix

Speakers List: Claudio Salmin, Tuukka Helander


Skills Requirements: above NSE-4 and VMware NSX knowledge

Duration: 4 hours

Data center security is being reshaped by virtualization, consolidation, and promising new technologies such as Software Defined Networking (SDN).

The adoption of the SDDC brings new challenges such as inspecting East-West traffic without the need to compromise on all the benefits of today’s physical appliances.

During this session you will learn how FortiGate-VMX enables greater security thanks to the full integration into VMware’s SDDC.

Products List: FortiGate-VMX
SECURITY AND PERFORMANCE ASSESSMENT

Level: Basic

Speakers List: Emmanuel Rabatan, Mike Strickland


Skills Requirements: NSE-4

Duration: 4 hours

In this 2 parts session we propose the attendees to discover two Fortinet products. The first is CTAP which allow you to assess for real the security of your network environment. The second is FortiTester that give you the power challenges the security effectiveness and the performance of your network security components.

- Part 1: most of the partners have heard about CTAP reports but they need to understand the real advantage of using it. CTAP with FortiSandbox adds a great value on the offer and this session will also include some comparisons with the competition.

- Part 2: in this part, we introduce Firewall performance and feature testing with FortiTester and configure network profiles and test cases to test Next-Gen Firewall features, including: Firewall, DDoS, IPSec, ATP, IPS and Application Control signatures.

Products List: FortiTester, FortiGate, FortiHypervisor, CTAP
**CAPTURE THE FLAG**

**Level:** Mix

**Speakers List:** Axelle Apvrille

**Technical Requirements:** Laptop with 8Go RAM and Wifi. Modern web browser. SSH/Telnet terminal client. Ethical hacking tools (i.e. Kali Linux virtual machine)

**Skills Requirements:** NSE-4

**Duration:** 4 hours

A capture the flag (CTF) contest is a special kind of cybersecurity competition designed to challenge its participants to solve computer security problems and/or capture and defend computer systems. Typically, these competitions are team-based but attendees are free to organize as they want.

In these sessions, the attendees will participate to Jeopardy-style competitions involving multiple categories of problems, each of which contains a variety of questions of different points values and difficulties. Teams/attendees attempt to earn the most points by completing as many cybersecurity challenges as they can from a given selection, testing their skills and knowledge on a diverse range of computer security categories.

Some of the CTF challenges will involve Fortinet products playing a role into the Security Fabric.

It will be short to complete challenges in one session. Please attend both if possible.

**Products List:** FortiAnalyzer, FortiClient, FortiGate, FortiMail, FortiSandbox, FortiSwitch, FortiWeb.