



**FORTINET**<sup>®</sup>  
Training Institute



# Introduction to Fortinet Network Security



# Introduction

# Cyber Threats

- Wide range of threats, from distributed denial-of-service (DDoS) attacks to ransomware
- Even a minor disruption can cause damage to an organization
- Cybercriminals adapt quickly to changing environments, like those that occurred during 2020

# Network Security

- Technologies, processes, and policies used to defend any network from cyberattacks, unauthorized access, and data loss
- Every organization requires network security to protect critical assets and infrastructure
- A layered approach protects both the network edge and everything inside the network
- Organizations should prioritize solutions that cover a multitude of threats



# The Fortinet Solution

# FortiGate Next-Generation Firewall

- Next-generation firewall (NGFW) enables security-driven networking, including security features such as:
  - Intrusion prevention system (IPS)
  - Web filtering
  - SSL inspection
  - Advanced threat protection (ATP)
- Uses information from FortiGuard Labs to stay ahead of the threat landscape
- Inspects traffic to prevent attacks without degrading the user experience
- As part of the Fortinet Security Fabric, a FortiGate can communicate with other Fortinet devices, as well as with third-party security solutions

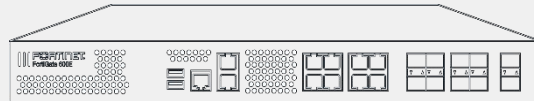
# FortiGate Portfolio Covers Small Branch to Hyperscale

Entry-Level Appliance  
FGT 30 – 90 Series

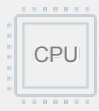


SOC Based

Mid-Range Appliance  
FGT 100 – 900 Series

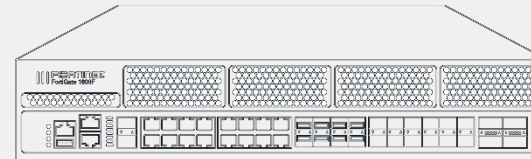


Network Processor

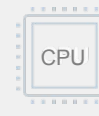


Content Processor

High-End Appliance  
FGT 1000 – 6000 Series



N x  
Network Processor

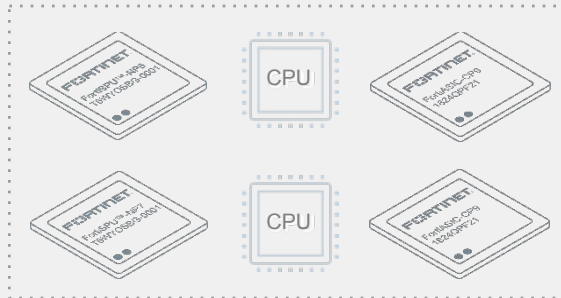
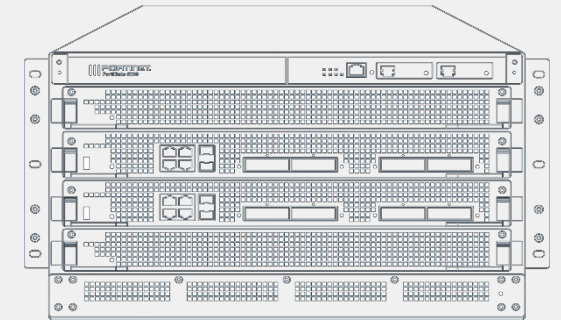


N x  
CPU



N x  
Content Processor

Chassis  
FGT 7000 Series



Blades

# Fortinet Security Fabric

## Broad

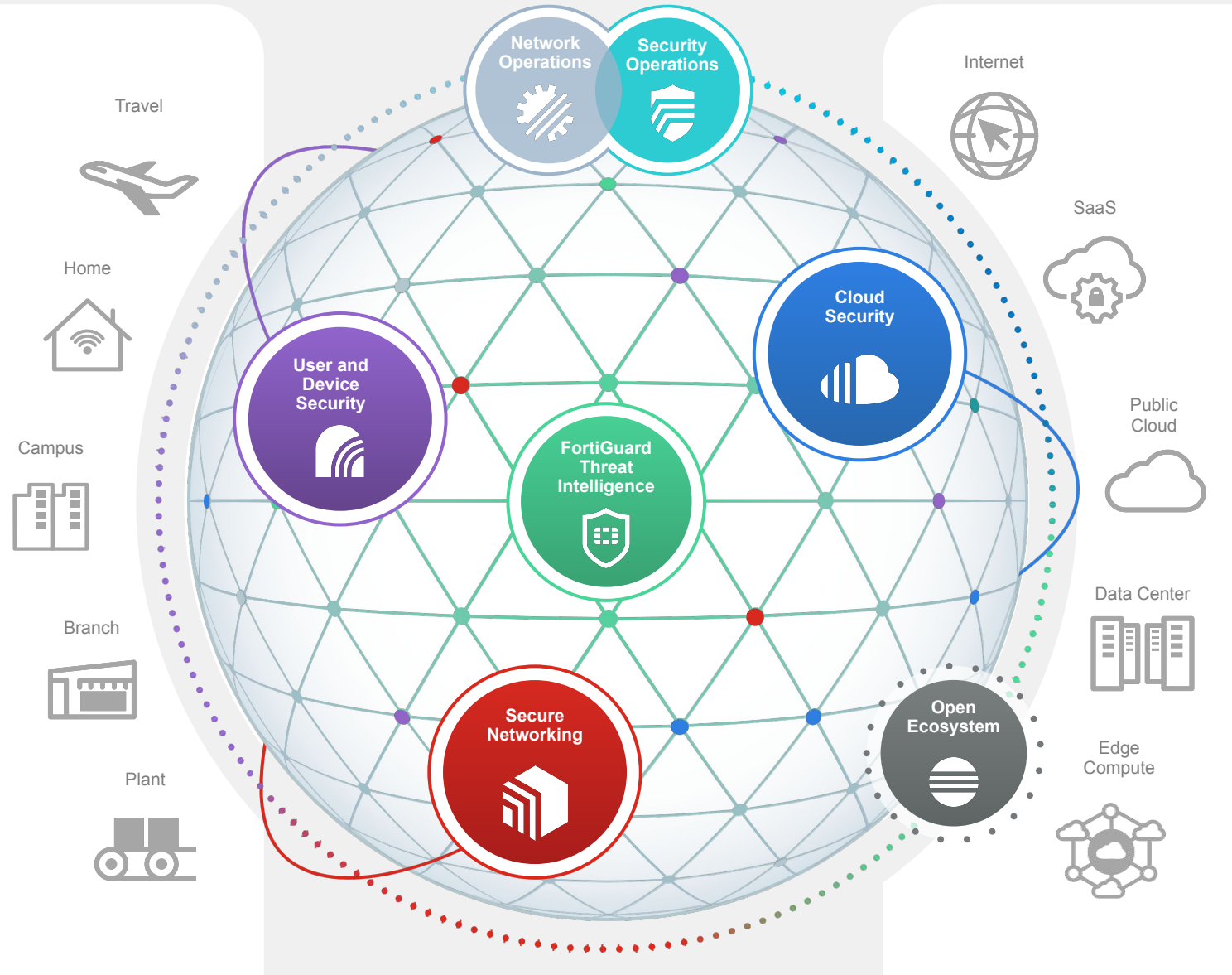
Visibility and protection of the entire digital attack surface to better manage risk

## Integrated

Solution that reduces management complexity and shares threat intelligence

## Automated

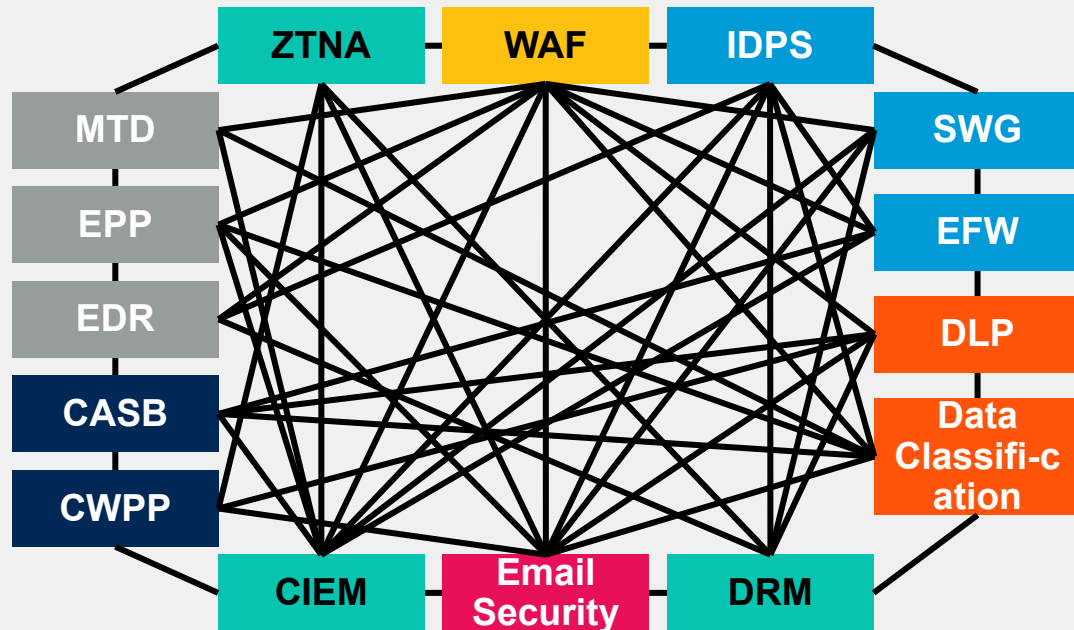
Self-healing networks with AI-driven security for fast and efficient operations





# Gartner Cybersecurity Mesh Architecture

Gartner®

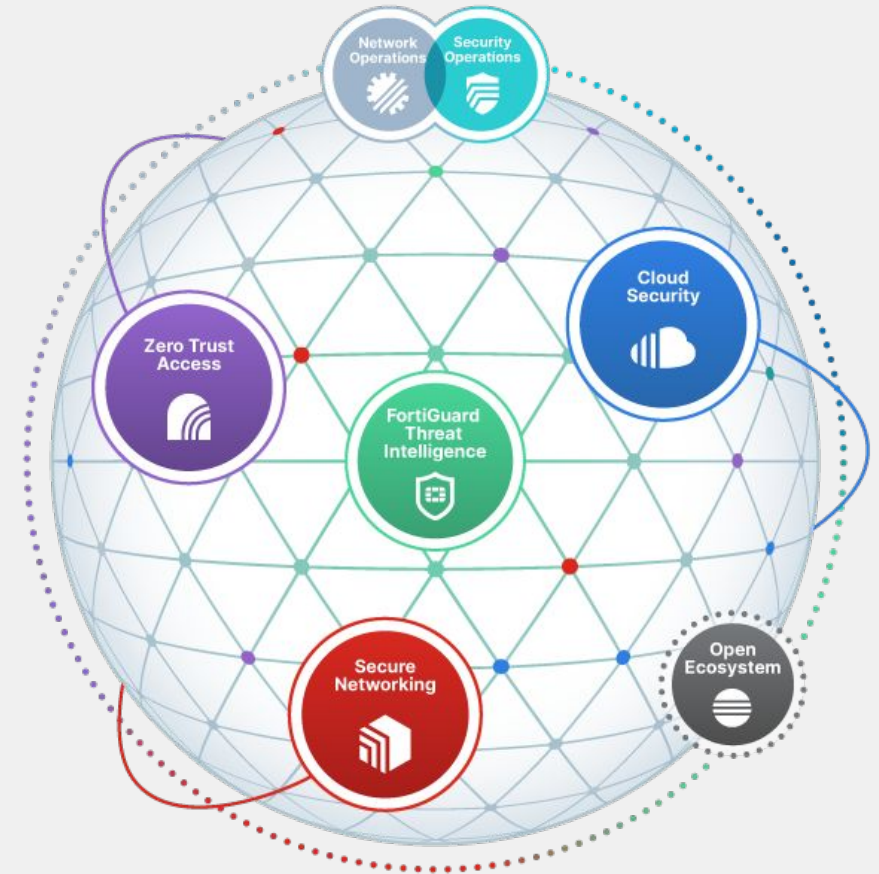


Executive Guide to Cybersecurity Mesh, 2022












Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET®



# FortiGuard Security Services

		Security-driven Networking			Adaptive Cloud				Fabric Management Center			Open Ecosystem	
		 FortiGate	 FortiProxy	 FortiClient	 FortiWeb	 FortiCASB	 FortiADC	 FortiMail	 FortiDoS	 FortiSandbox	 FortiAnalyzer	 FortiSIEM	Developer network and open ecosystem
Content Security	AV	●	●	●	●	●	●	●		●			
	Sandbox Cloud	●		●	●			●					
	Credential Defense				●								
	DLP Native (not a service)	●	●										
	Virus Outbreak	●						●					
	Anti-Spam		●					●					
Web Security	IP Rep	●			●		●		●	●			
	Web and Video Filtering	●	●	●			●			●			
	Botnet DB	●		●	●	●	●						
	Geo IP	●		●	●								
	DNS	●	●										
	Web Application				●		●						
Device Security	Vulnerability Scan		●	●	●								
	IPS	●	●	●			●			●			
	IoT mac to vendor mapping	●											
	IoT real time query	●											
	OT detection and protection	●											
	Device/OS detection	●											
	IoC										●	●	●

# Gartner 2022 Magic Quadrant for Network Firewalls

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

## Fortinet recognized for Network Firewalls for the 13th time

*Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hills, Tom Lintemuth, 19 December 2022*

*GARTNER is a registered trademarks and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.*

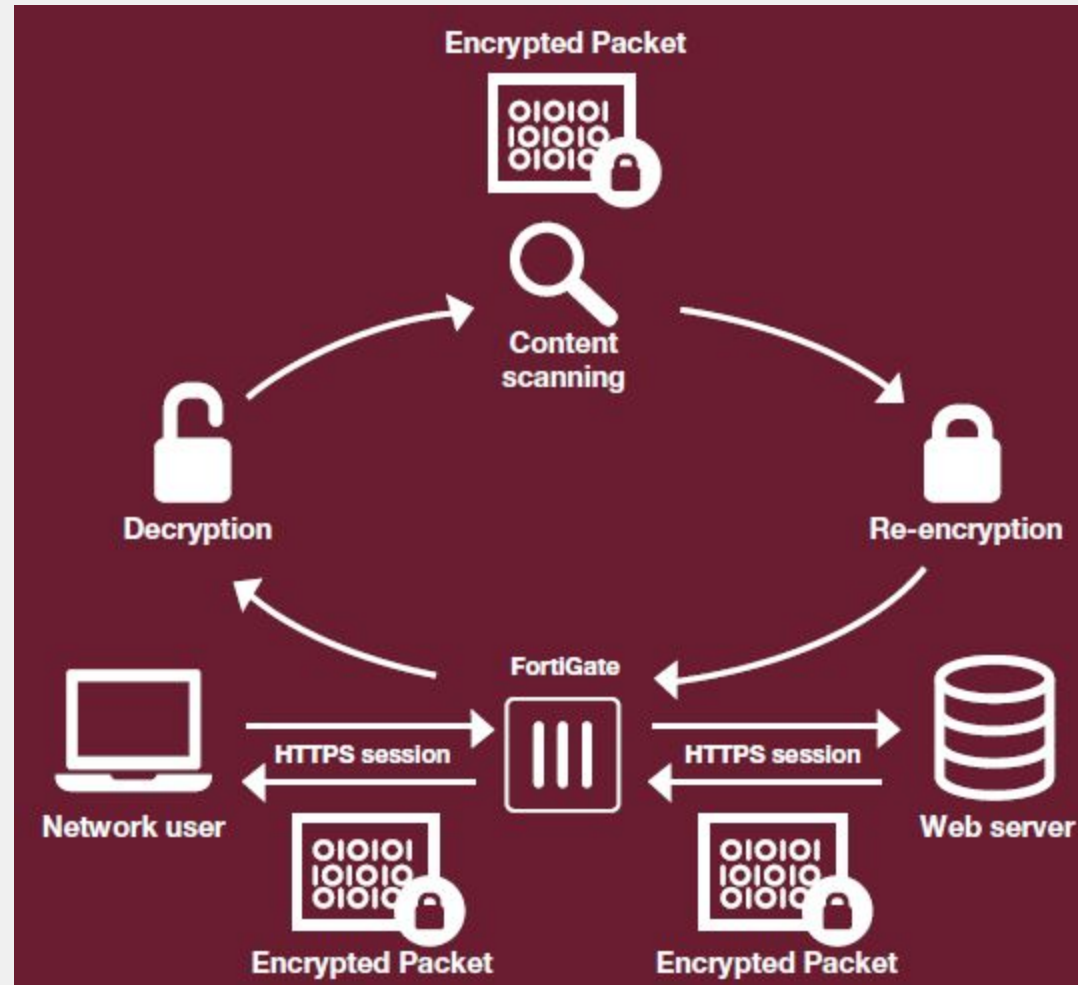
*This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.*

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

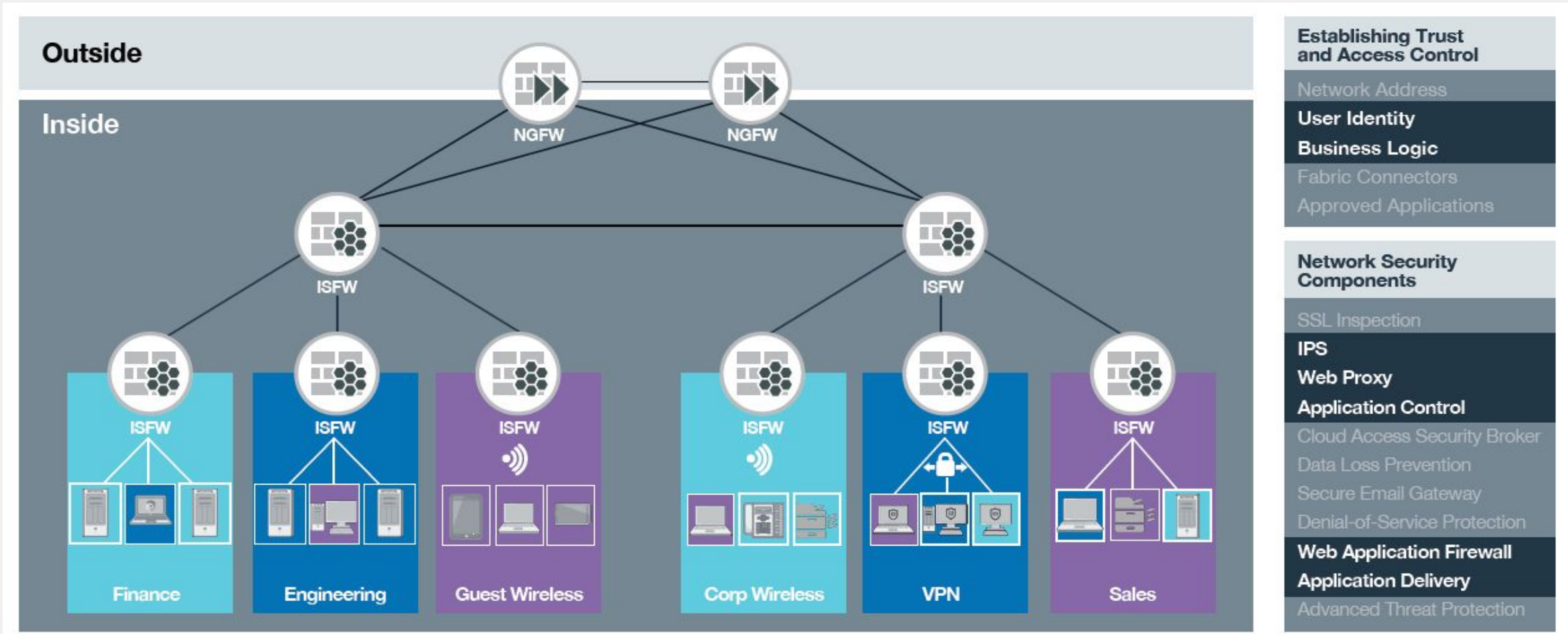


# Use Cases

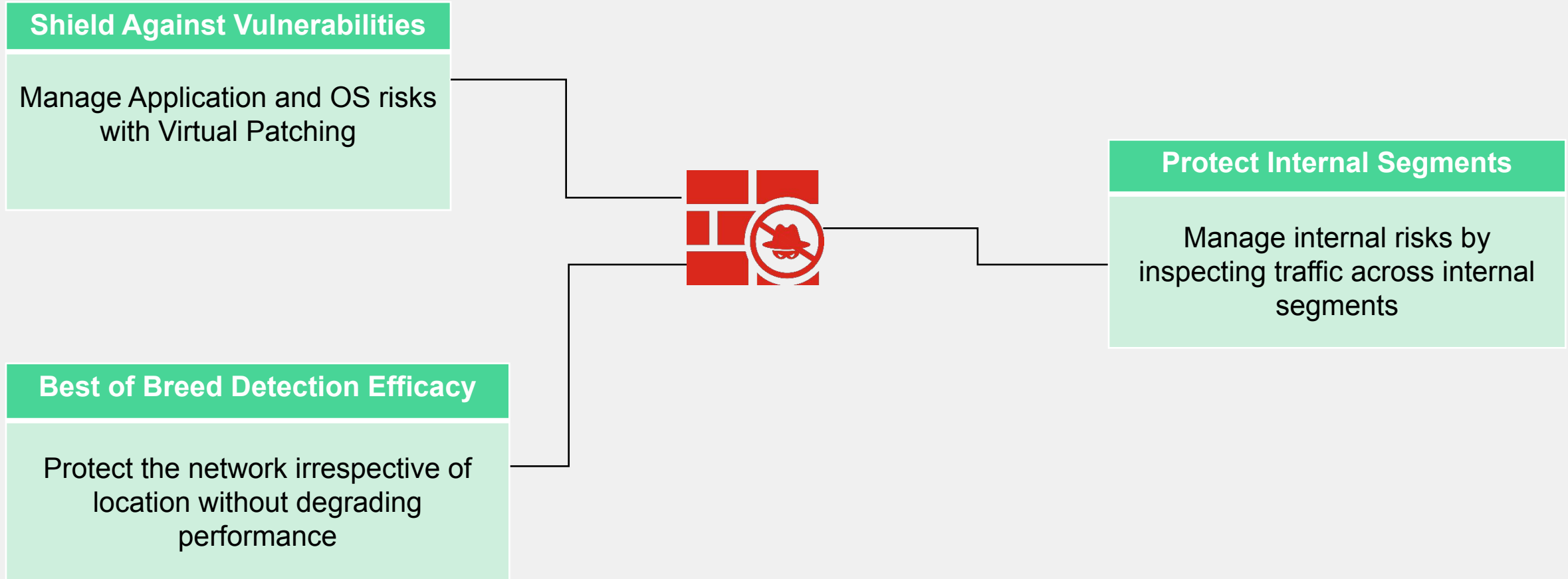
# Manage External Security Risks



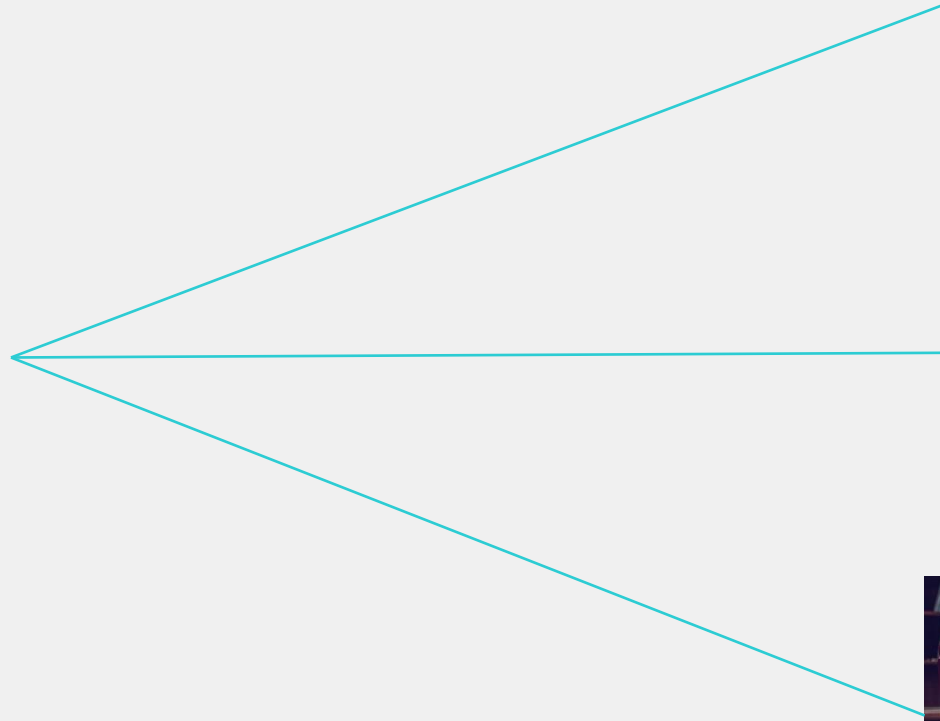
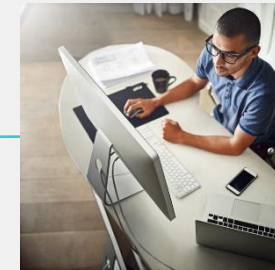
# Manage Internal Security Risks



# Manage Vulnerabilities



# VPN Solution








# Enabling Technologies

# Configuring Interfaces


- Assigning IP addresses:
  - Manually
  - Automatically (DHCP or PPPoE)
- Interface roles:
  - LAN
  - WAN
  - DMZ
  - Undefined
- Use aliases to keep track of each interface


## Network > Interfaces

### Edit Interface

Name  port8

Alias

Type  Physical Interface

Role  Undefined

#### Address

Addressing mode  Manual  DHCP  One-Arm Sniffer

Retrieve default gateway from server

Distance

Override internal DNS

# Routing

- Should be at least one default gateway
- If the interface is DHCP or PPPoE, the route and gateway can be added dynamically
- This might also be provided by a dynamic routing protocol such as OSPF, RIP, IS-IS, or BGP

## Network > Static Routes

New Static Route

Destination ⓘ **Subnet** Internet Service  
0.0.0.0/0.0.0.0

Gateway Address  
10.200.2.254

Interface  
port2

Administrative Distance ⓘ  
10

Comments  
Write a comment... 0/255

Status  
**Enabled** Disabled

Advanced Options

Priority ⓘ 0

**OK** Cancel

# Firewall Policies

- Policies define:
  - Which traffic matches
  - How to process matching traffic
- When a new IP session packet arrives, the FortiGate:
  - Starts at the top of the list to look for a policy match
  - Applies the first matching policy
  - If no policies match, the FortiGate applies implicit deny policy and traffic is dropped

## Policy & Objects > Firewall Policy

LAN (port3) → ISP1 (port1) 1												
2	Internet_Access_ISP1	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled	PRX default	AV default	WEB default	SSL deep-inspection	All
LAN (port3) → ISP2 (port2) 1												
3	Internet_Access_ISP2	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled	PRX default	AV default	WEB default	SSL deep-inspection	All
Implicit 1												
0	Implicit Deny	all	all	always	ALL	DENY	Disabled					Disabled

# Security Profiles

- Antivirus
  - What do to when an infected file is detected
  - Whether scanning is flow-based or proxy-based
  - Which protocols to inspect
  - Advanced persistent threat (APT) protection options, including sandboxing
  - Virus outbreak prevention options
- Web filtering
  - Determines the action to apply when a user tries to browse to a specific website
  - Flow-based or proxy-based
  - FortiGuard category-based filtering
  - Static URL filters
- Application control
  - Determines the action to apply when a user tries to use a specific application
  - Three types of filters: categories, application overrides, and filter overrides

# Logging

- Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response (if any)
- Event logs record system and administrative events, such as adding or modifying a setting, or daemon activities
- Security logs record security events, such as virus attacks and intrusion attempts, based on the security profile type
  - If no security logs exist, the menu item does not appear in the GUI

# Authentication

- Local authentication
  - Username and password stored on the FortiGate
- Remote authentication
  - Password stored on a POP3, RADIUS, LDAP, or TACACS+ server
- Two-factor authentication
  - Enabled on top of an existing method
  - Requires something you know and something you have (token or certificate)
- Guest authentication
  - User accounts that expire after a predetermined amount of time

# Using the CLI

- Connect to the CLI:
  - CLI console button in the GUI
  - Drop-down menu available in the GUI for certain objects
  - Connecting via SSH using a terminal emulator application
  - Console or USB management port
- Basic CLI commands:
  - config: Configure objects and system settings
  - get: Get information about the current configuration
  - show: Show the configuration
  - diagnose: Diagnose system status to troubleshoot network problems
  - execute: Execute static commands



# SSL VPN

- A VPN extends a private network across a public network
- SSL VPN on FortiGate supports two modes:
  - Web mode: remote users connect using a web browser
  - Tunnel mode: remote users connect using FortiClient

# SSL VPN (Contd)

## Web Mode

- Remote users establish a secure connection between the the web browser and the SSL VPN portal, using HTTPS
- Once connected, users provide credentials in order to pass an authentication check
- The FortiGate displays the SSL VPN portal, which contains services and network resources for users to access

## Tunnel Mode

- Users connect to FortiGate through FortiClient
- Users provide credentials to successfully authenticate
- The FortiGate establishes the tunnel and assigns an IP address to the client. This is the client's source IP address for the duration of the connection
- Users can access services and network resources through the encrypted tunnel



# Conclusion

# To Learn More

Consider taking the following NSE Training courses to get a deeper understanding on the products covered in this workshop:

- FortiGate Security
- FortiGate Infrastructure

# Fortinet Training Institute

## Certification Program

840,000+ Certifications

Levels	Certifications
Fortinet Certified Expert	
Fortinet Certified Solution Specialist	
Fortinet Certified Professional	
Fortinet Certified Associate	
Fortinet Certified Fundamentals	

## Authorized Training Centers

Supporting language and culture in training in 134 countries and territories

## Education Outreach Program

- Work with global leaders to drive change
- Focused on veterans, women and other underrepresented populations
- Partnerships extend to industry, academia, government and non-profits
- Removes barriers to training and education with > \$40M in free training



IBM SkillsBuild



## Veterans Program

- Partner with military focused non-profits to help over 2500 veterans and military family members
- Connect graduates with Fortinet employer ecosystem
- Brings untapped candidates into the cyber-workforce



## Security Academy Program

- Range from K-12 to higher education and research institutions
- Institutions integrate NSE Certification Program content into curriculum
- Provides free exam vouchers to promote certifications

**+439**  
Institutions

**+94**  
Countries and Territories

## Awards



<https://www.fortinet.com/nse-training/training-program-update>

# Fortinet Fast Track Training Qualifies for (ISC)2 Credits

- Earn 1 credit for every hour of Fast Track training, up to 8 hours per day, towards maintaining your CISSP certification.
- Log into your (ISC)2 CPE Portal to claim your credits:
  - Approximately 24 hours after you complete the workshop, you can download the course completion certificate at <https://training.fortinet.com>
  - Course Name: Introduction to Fortinet Network Security
  - Number of training hours: 4 hours
  - (ISC)2 CISSP Domain 4: Communication and Network Security
  - Provide the date you completed the training

# Fast Track Lab

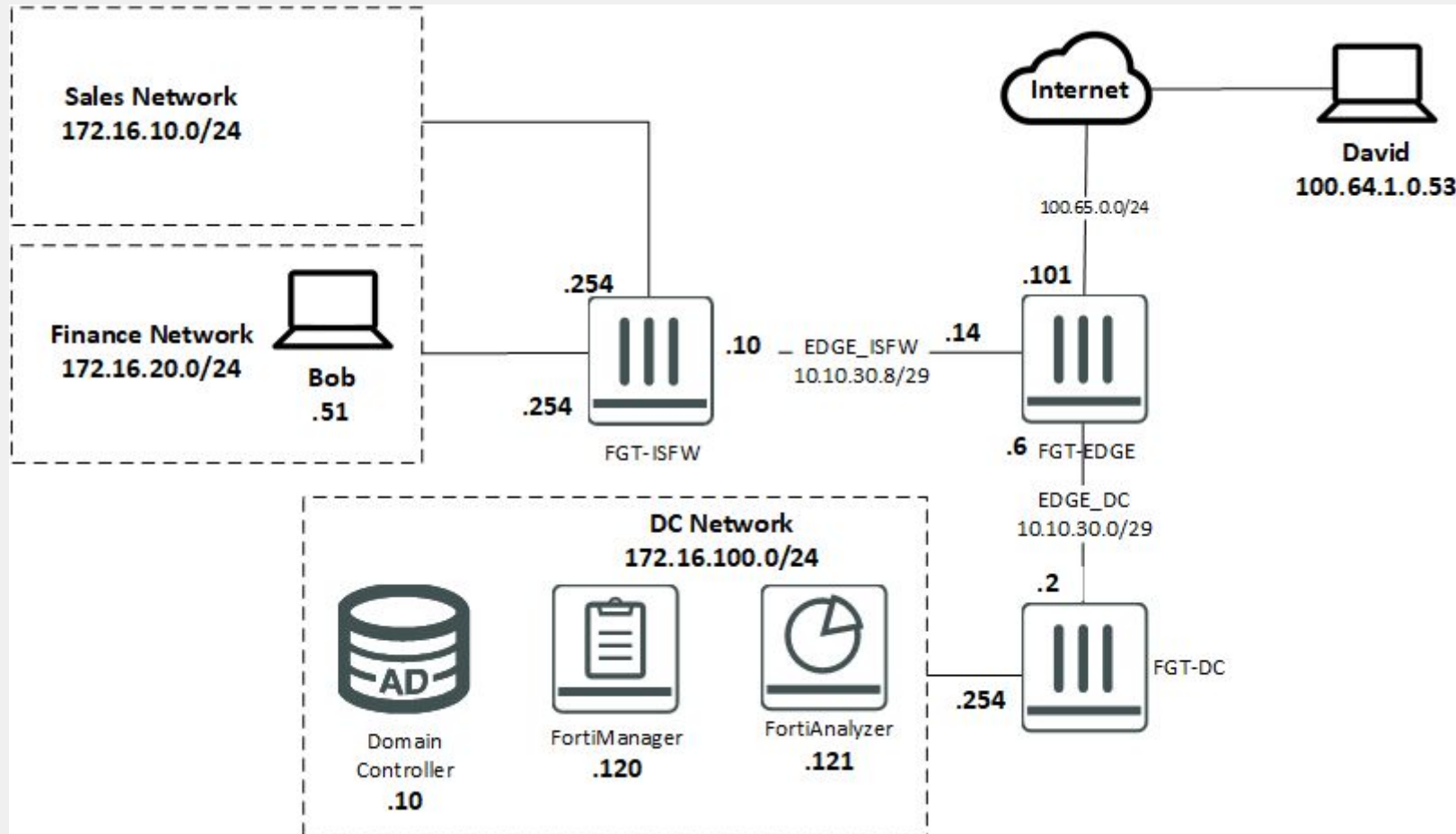
Link to labs

<https://training.fortinet.com/course/view.php?id=56305>

Enrollment Code:

**dbc687351c**

# Network Diagram





**FORTINET®**