FORTINET®

CONSTRUCTING A SECURE SD-WAN ARCHITECTURE

Constructing a Secure SD-WAN Architecture

SD WAN

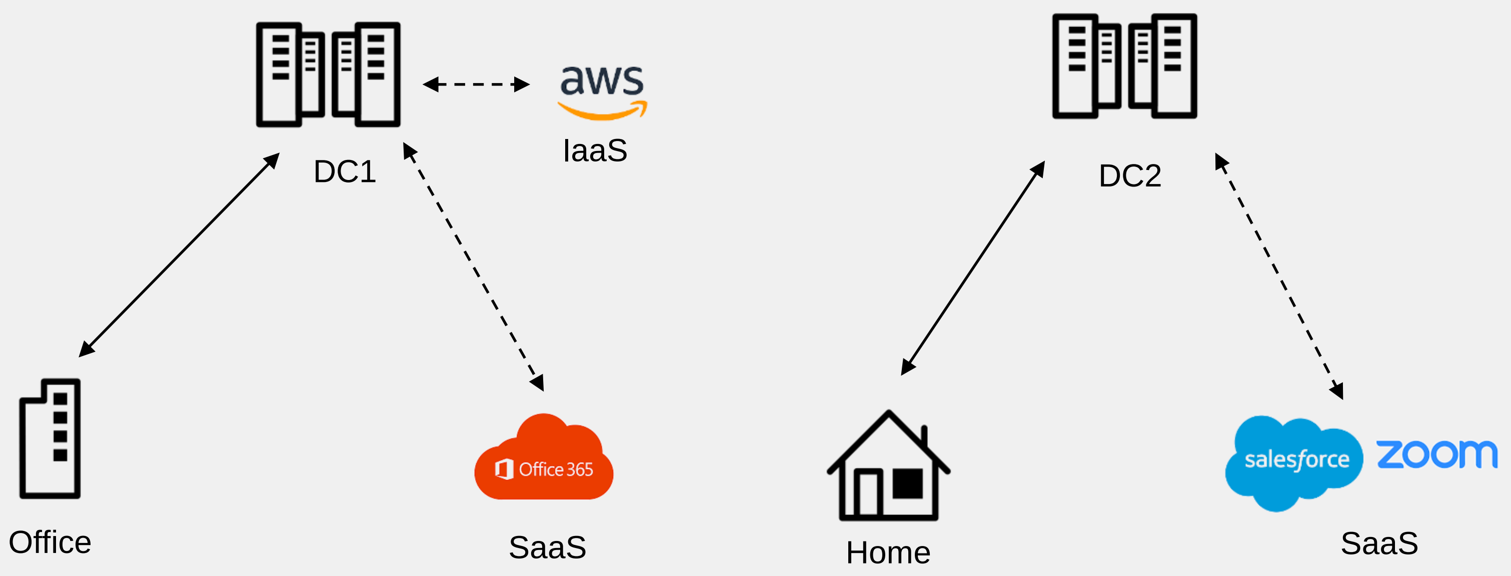
Objectives

- Understanding SD-WAN Trends and Challemges
- Fortinet Secure SD-WAN
- Secure SD-WAN use cases
- SD-WAN Assessment Program
- Customer Success Stories
- Configuring Secure SD-WAN

Understanding WANEdge Trends & Challenges

Traditional WAN Impacts User Productivity

Creating Obstacles for Digital Innovations

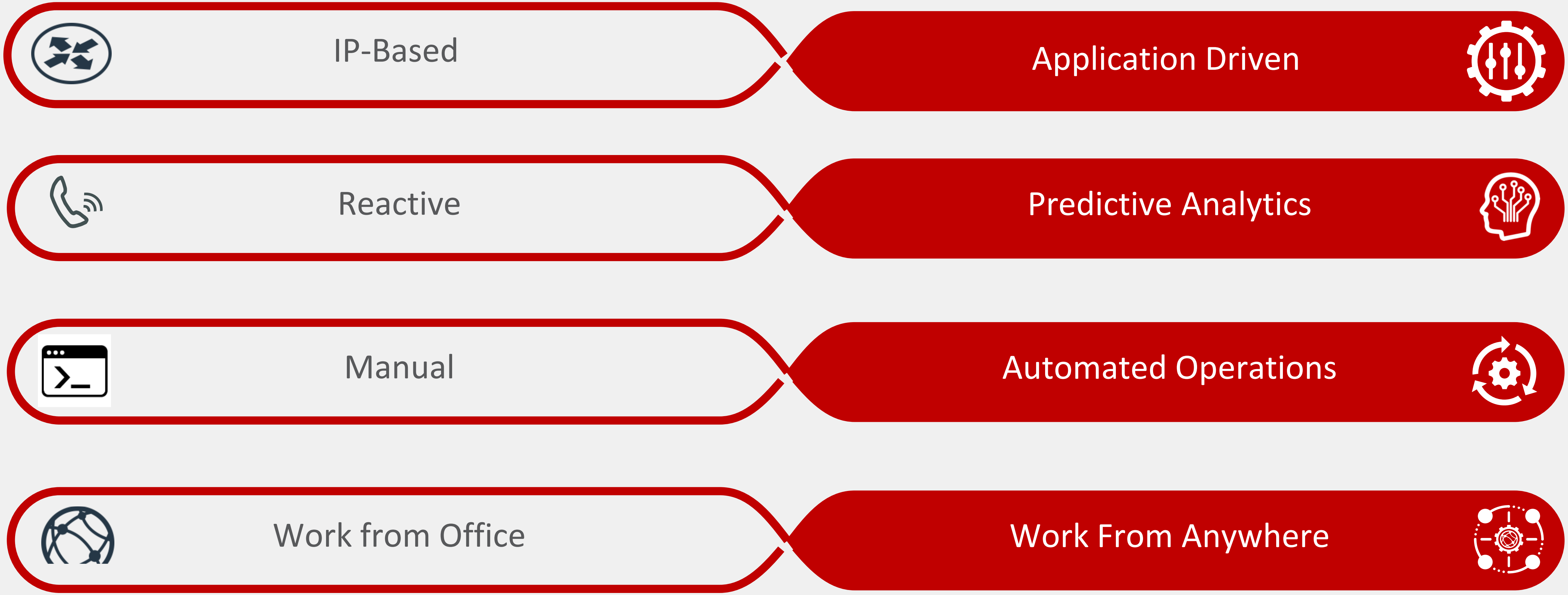


Hybrid Workforce and lack of Modern Infrastructure

Main Challenges

- Poor User Experience
- High WAN Cost
- Complex Operations

The Network Transformation Trends



IP-Based	Application Driven
Reactive	Predictive Analytics
Manual	Automated Operations
Work from Office	Work From Anywhere

Business Value of Moving to SD-WAN

01 **Improve User Experience**

Direct internet access for business applications instead backhauling to HQ

02 **Instant ROI Benefits**

More bandwidth for users, consolidate networking and security point products

03 **Simplified Operations**

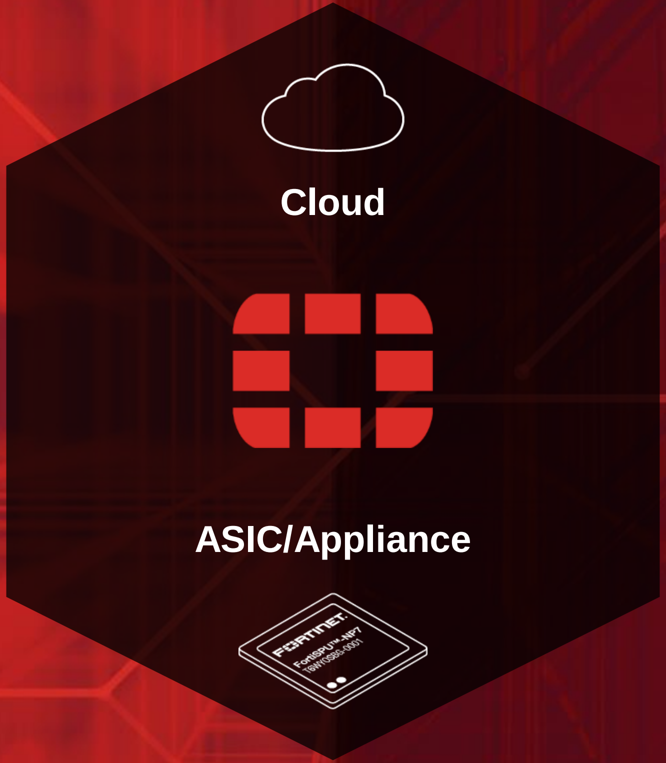
Enhance business agility with end-to-end visibility and automation

Fortinet Secure SD-WAN

Security-Driven Networking

The Next Era of Networking and Security Convergence

WIDE AREA NETWORKING



NETWORK SECURITY

Flexible, anywhere and anytime security

Fortinet’s Comprehensive Secure SD-WAN Solution

Industry’s leading Organically developed Secure SD-WAN Solution

01 **Application Driven**

Broadest application steering with accurate identification for better user experience

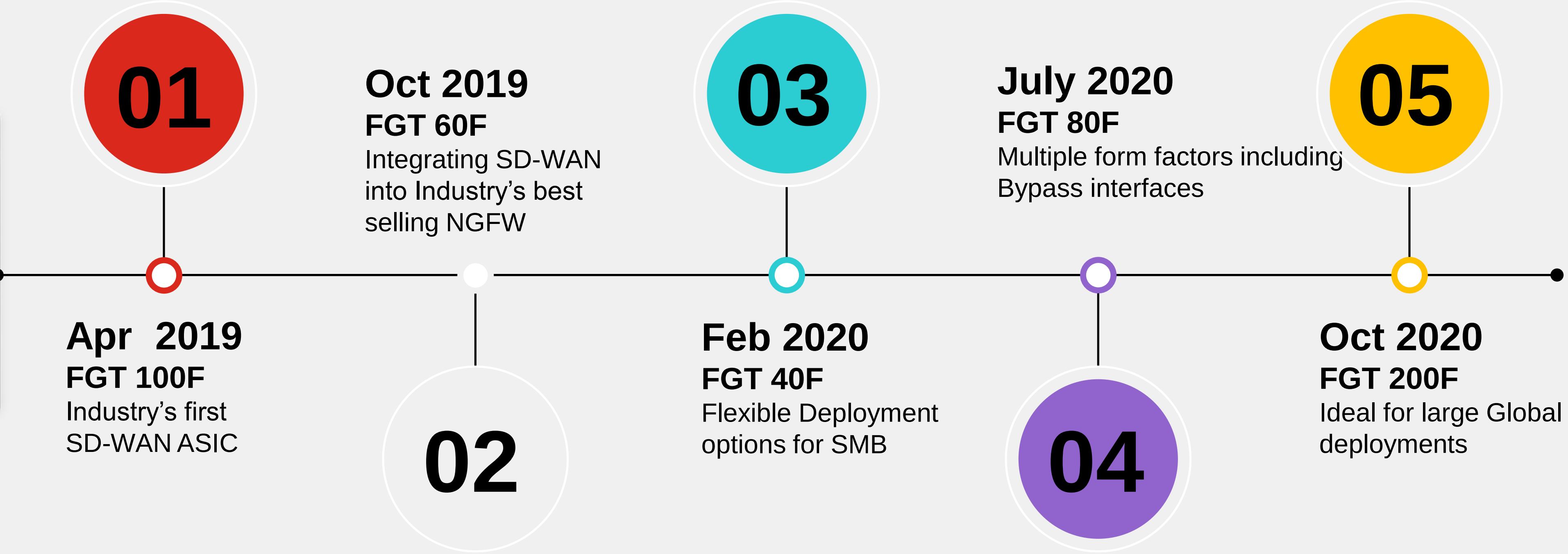
02 **Accelerated Convergence**

Industry’s only SD-WAN ASIC powered WAN Edge with advanced routing, SD-WAN and NGFW for flexible deployments

03 **Efficient Operations**

Centralized orchestration and analytics with end-to-end scalable ZTP for SD-WAN and SD-Branch

High-performing Portfolio powered by SD-WAN ASIC



Apr 2019
FGT 100F
Industry's first
SD-WAN ASIC

Oct 2019
FGT 60F
Integrating SD-WAN
into Industry's best
selling NGFW

Feb 2020
FGT 40F
Flexible Deployment
options for SMB

July 2020
FGT 80F
Multiple form factors including
Bypass interfaces

Oct 2020
FGT 200F
Ideal for large Global
deployments

Multiple variants
for every deployment

Built-in LTE

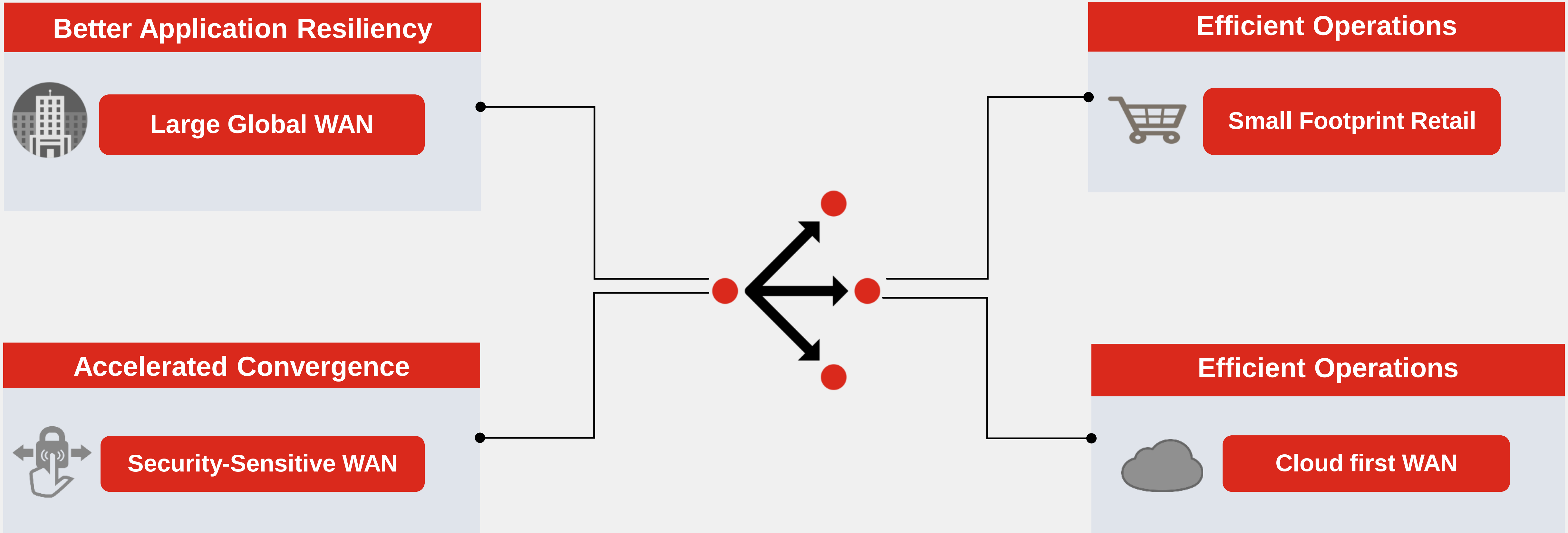
Built-in Wireless

Built-in POE

Built-in Bypass

Secure SD-WAN Use cases

Fortinet Secure SD-WAN Leading Use-cases



Better Application Resiliency

Large Global WAN

Accelerated Convergence

Security-Sensitive WAN

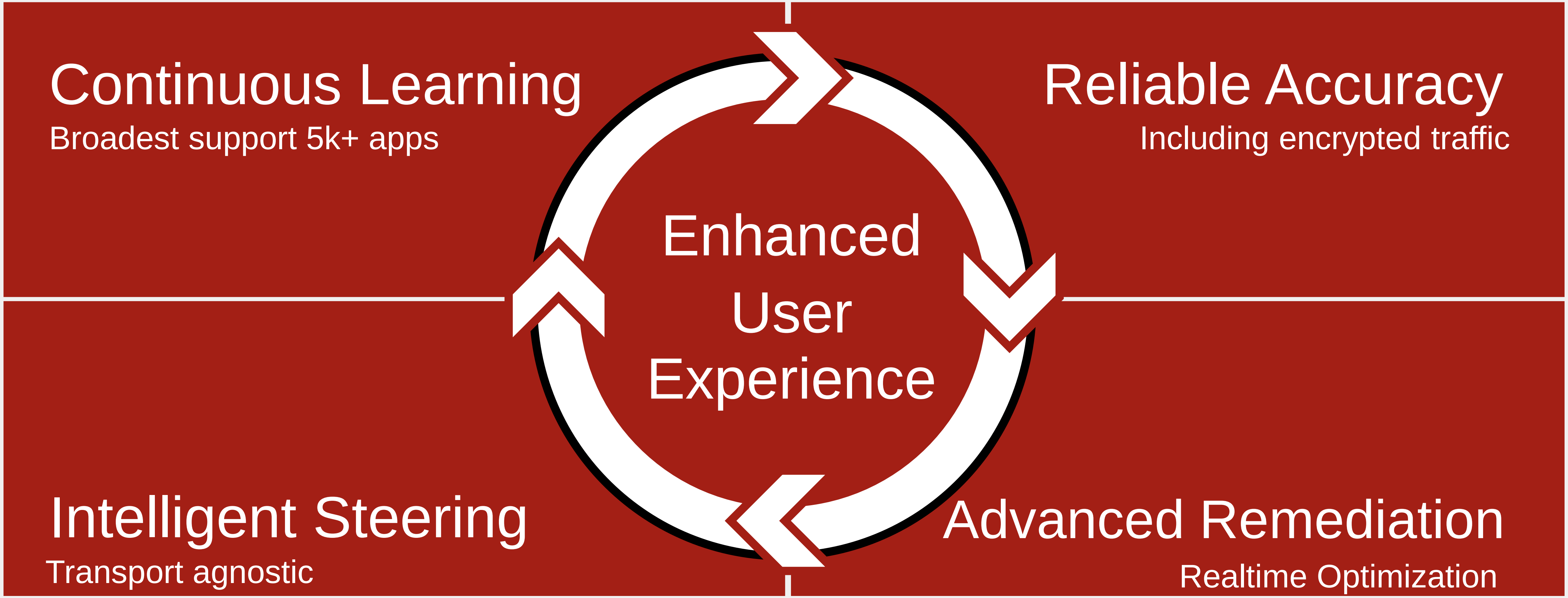
Efficient Operations

Small Footprint Retail

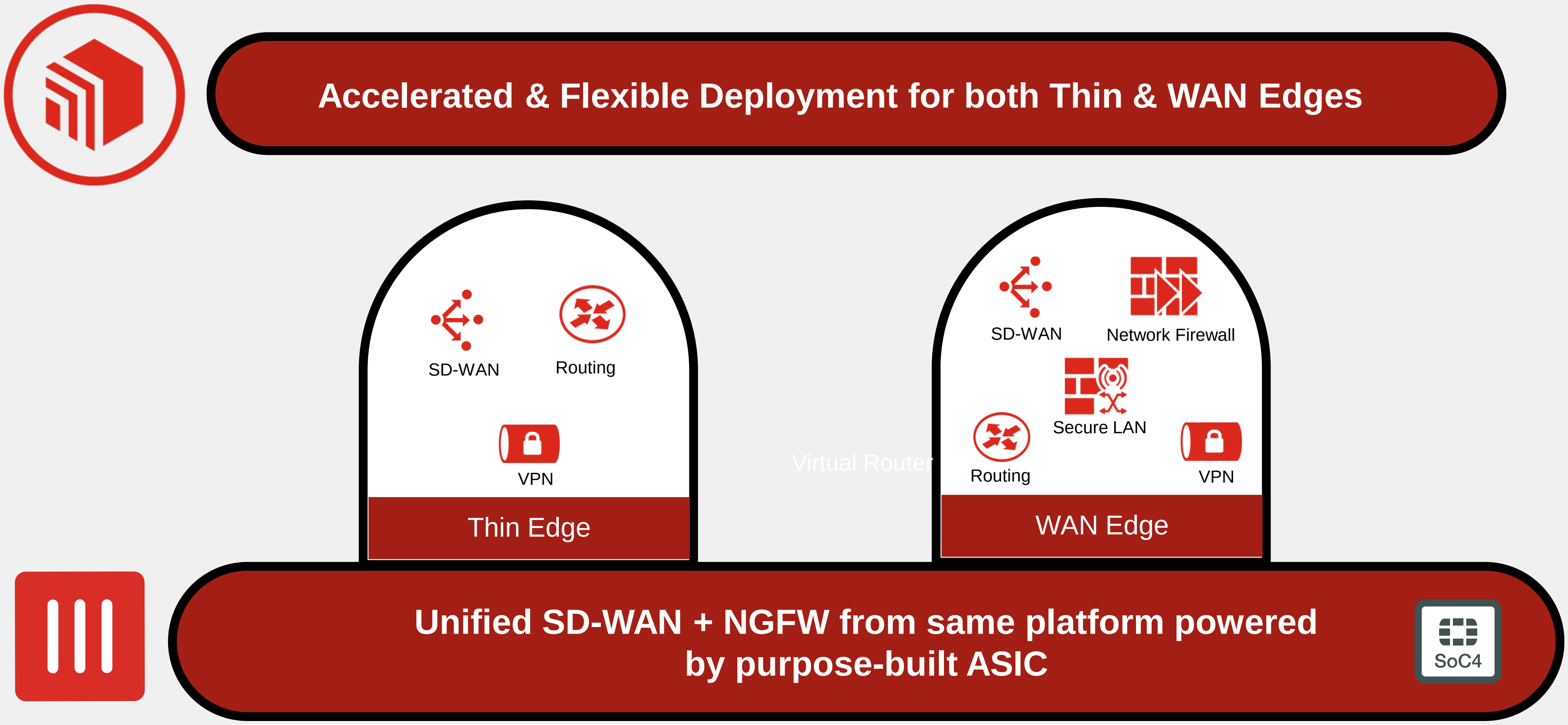
Efficient Operations

Cloud first WAN

Enabling Application Driven Networks



Accelerated Convergence for every Network Edge



Accelerated & Flexible Deployment for both Thin & WAN Edges

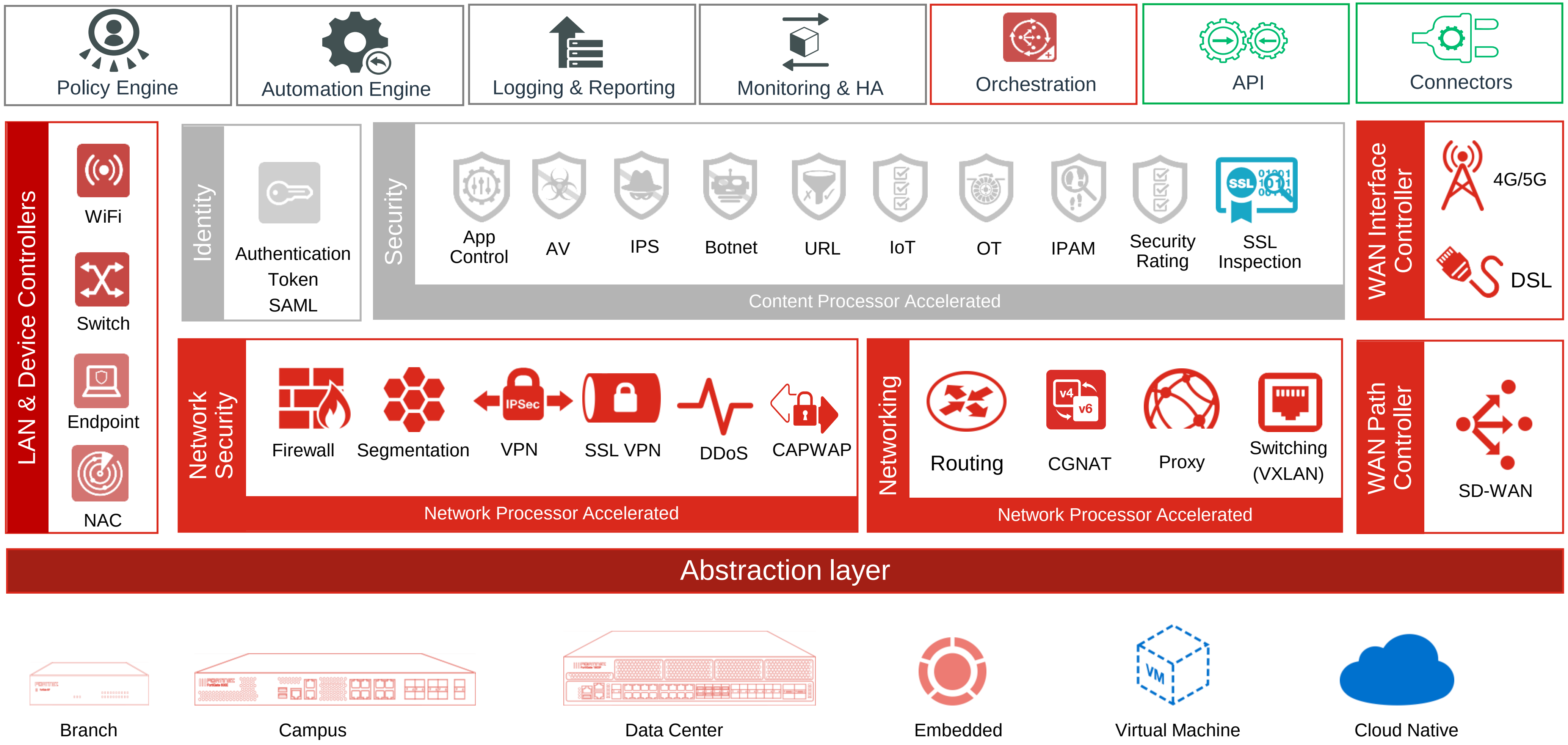
Thin Edge
- SD-WAN
- Routing
- VPN

Virtual Router

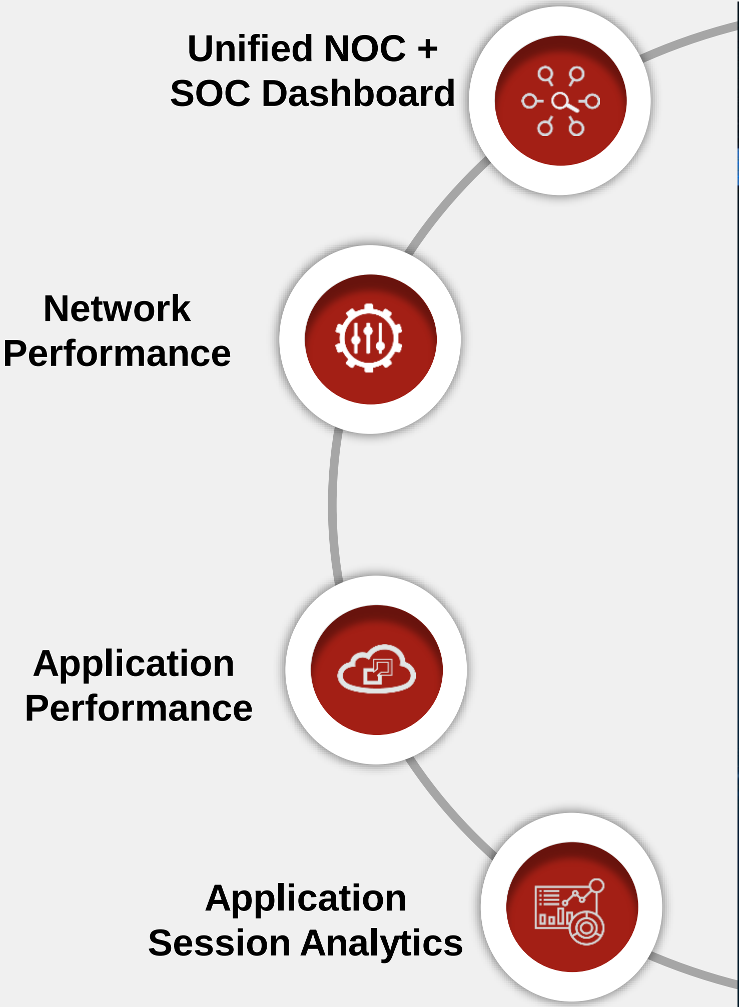
WAN Edge
- SD-WAN
- Network Firewall
- Secure LAN
- Routing
- VPN

Unified SD-WAN + NGFW from same platform powered by purpose-built ASIC

FortiOS Innovative Network Operating System



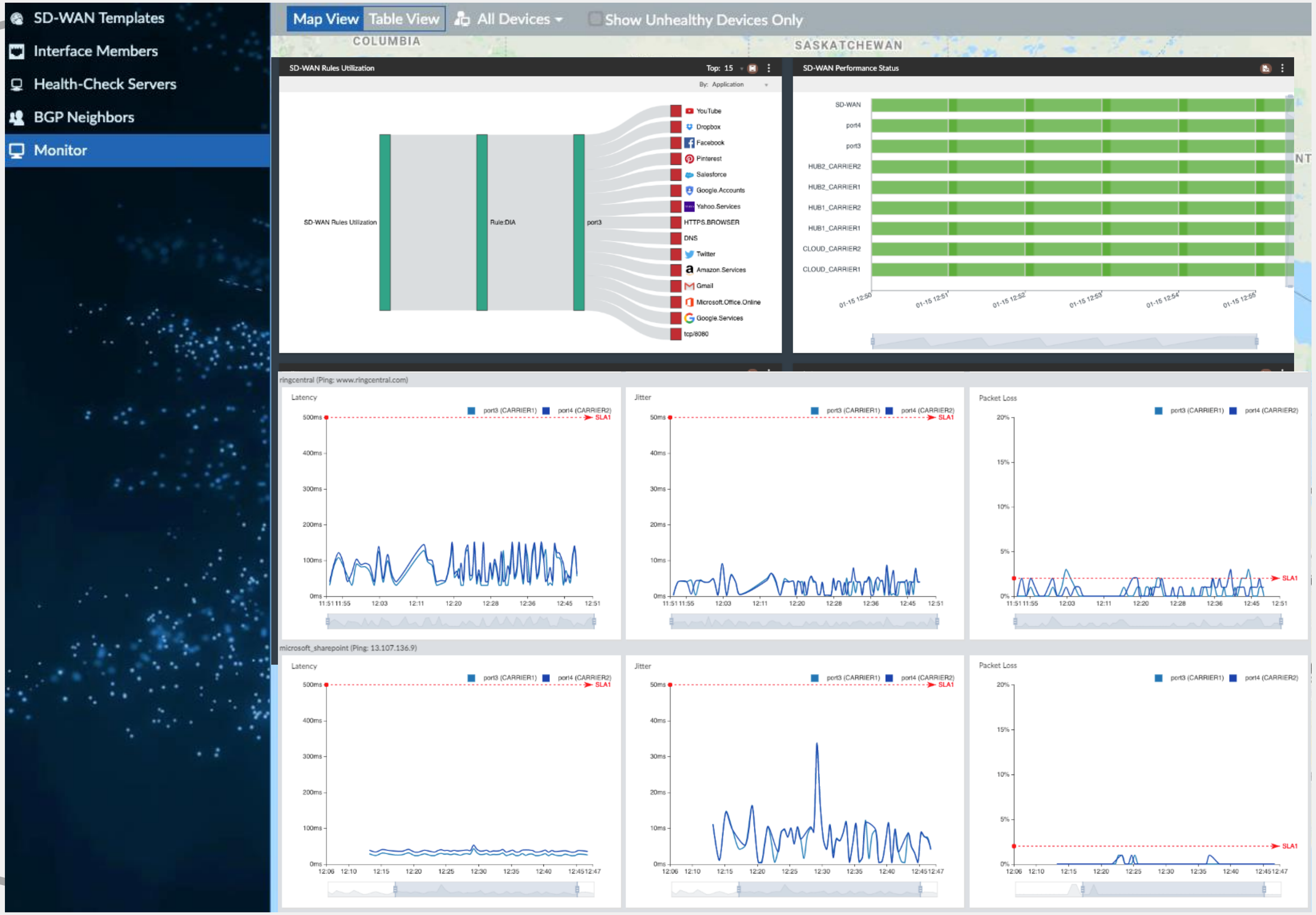
Efficient Operations with Centralized Management


Unified NOC + SOC Dashboard

Network Performance

Application Performance

Application Session Analytics

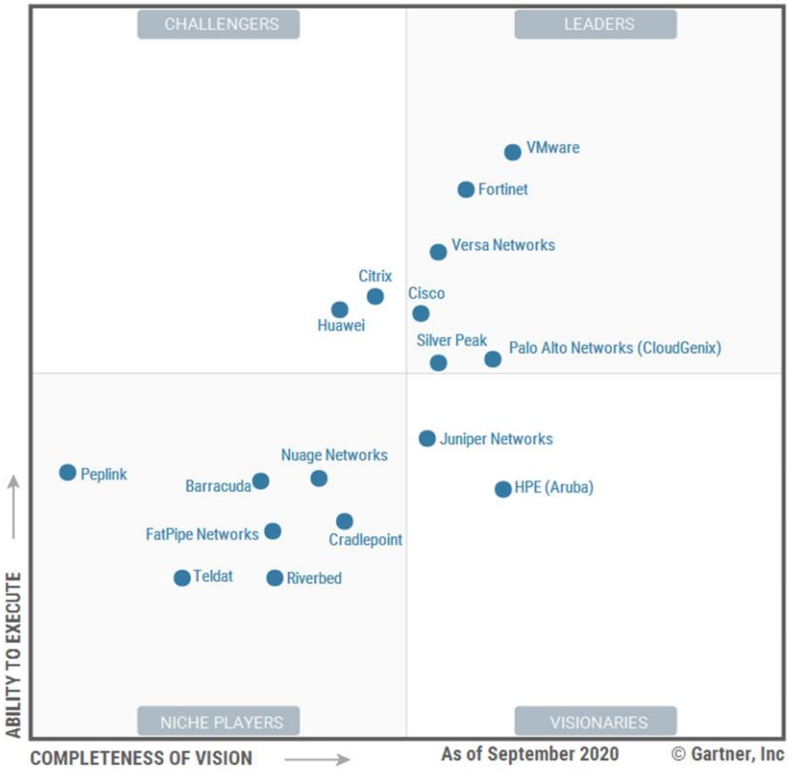


Fortinet SD-WAN Validation

Recognized As a Leader for Network Firewalls and WAN Edge Infrastructure

2020 Magic Quadrant for WAN Edge Infrastructure

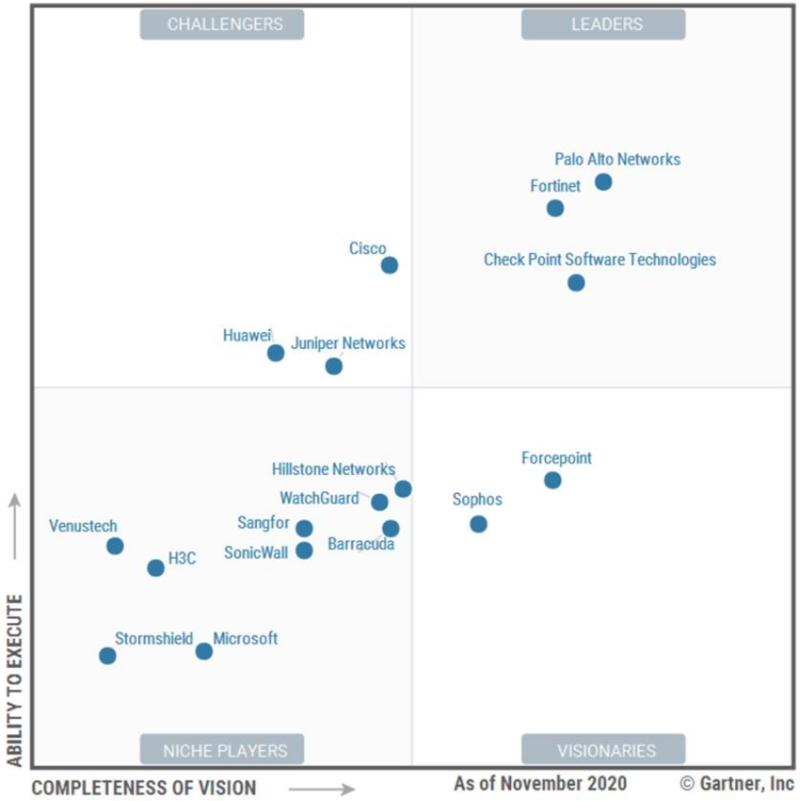
Figure 1. Magic Quadrant for WAN Edge Infrastructure



Source: Gartner (September 2020)

2020 Magic Quadrant for Network Firewalls

Figure 1. Magic Quadrant for Network Firewalls

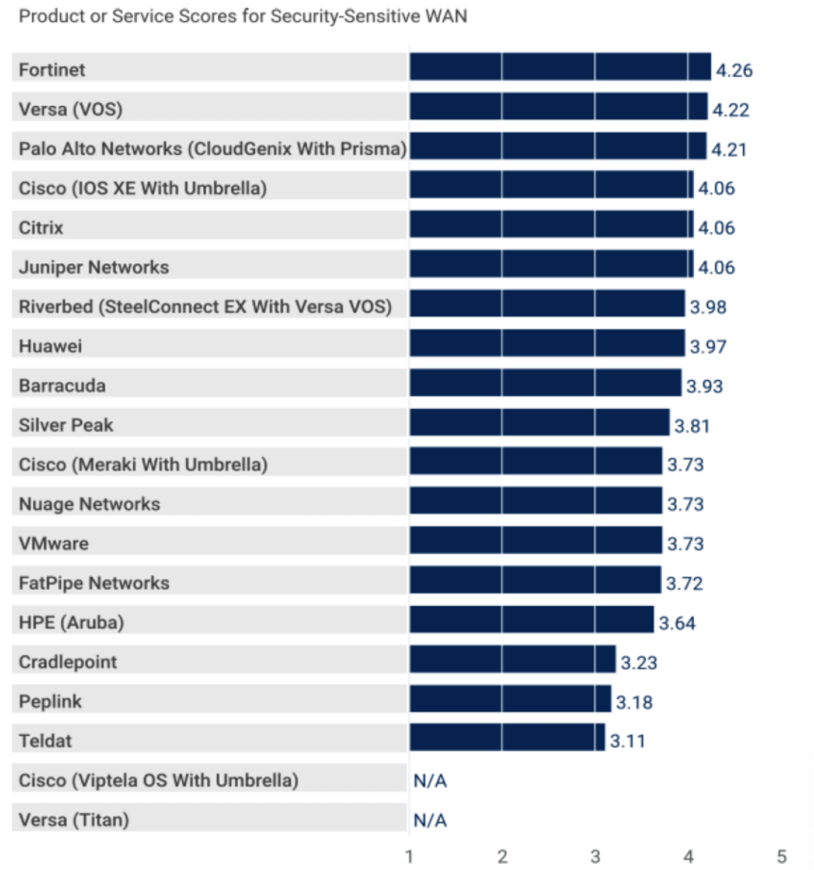


Source: Gartner (November 2020)

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.

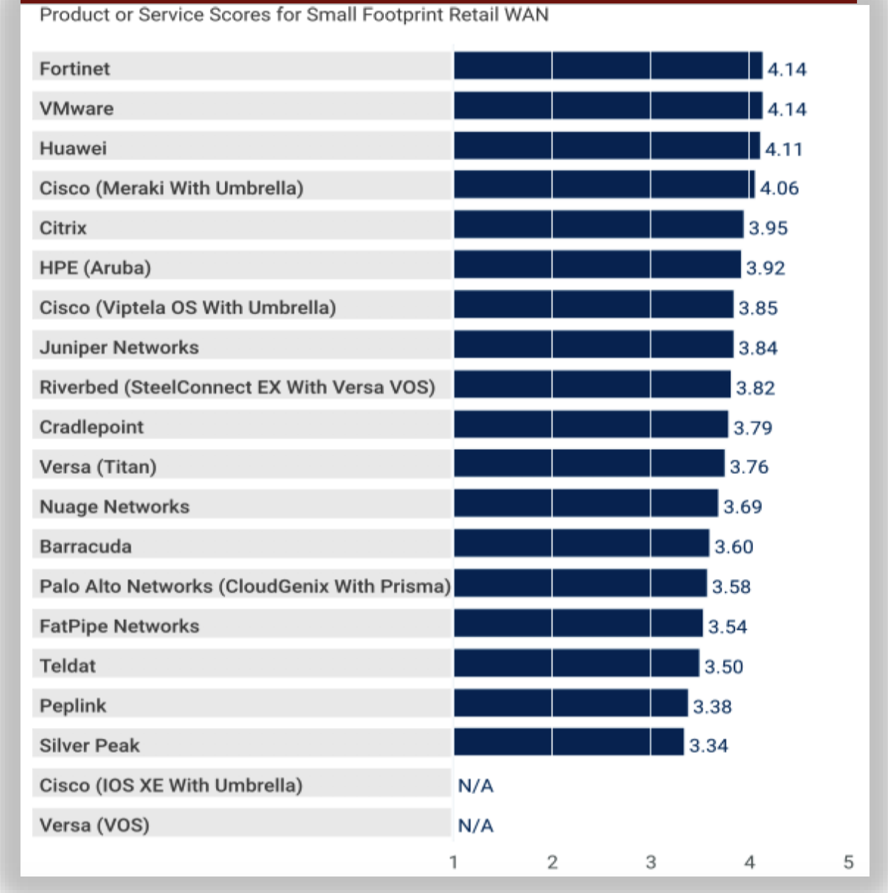
Gartner’s Critical Capabilities for WAN Edge Infrastructure

Security-Sensitive WAN Use-case



Fortinet is ranked **Highest** in the Security-Sensitive WAN and Small Footprint Retail WAN Use Cases

Small Footprint Retail Use-case



Gartner Critical Capabilities for WAN Edge Infrastructure, Jonathan Forest, Mike Toussaint, Mark Fabbi, 30 September 2020

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.

A Gartner Peer Insights Customers' Choice™

Highest Customer Reviews Received for WAN Edge Infrastructure Segment

Voice of the Customer

Ranked among Businesses across Industries, Regions and sizes

4.7/5 Rating   339 Reviews

Overall Rating
Number of Reviews

Gartner
peerinsights
customers'
choice
2021
TM

The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Customer Success

Global SD-WAN Customer Success Examples

WASTE MANAGEMENT

- **Fortune 500 – Large Enterprise**
- 1200 locations in North America
- 65% Cost reduction with consolidation
- Deployed sites in 9 months with ZTP

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

ROLLINS

- **Global 1000 – Large Enterprise**
- 700 locations in 50 Countries
- 10X Improved user experience
- 50%+ reduced network set-up time

Fortinet won against

- *Cisco ISR Router*
- *VMWARE VeloCloud, Versa*

Petrol Ofisi

- **1800 locations in Europe**
- 50% reduction in MPLS cost
- 99% increased business continuity
- Expanded to SD-Branch

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

Global SD-WAN Customer Success Examples

WM WASTE MANAGEMENT®

- **Fortune 500 – Large Enterprise**
- 1200 locations in North America
- 65% Cost reduction with consolidation
- Deployed sites in 9 months with ZTP

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

ROLLINS®

- **Global 1000 – Large Enterprise**
- 700 locations in 50 Countries
- 10X Improved user experience
- 50%+ reduced network set-up time

Fortinet won against

- *Cisco ISR Router*
- *VMWARE VeloCloud, Versa*

PO Petrol Ofisi

- **1800 locations in Europe**
- 50% reduction in MPLS cost
- 99% increased business continuity
- Expanded to SD-Branch

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

Global SD-WAN Customer Success Examples

WM

WASTE MANAGEMENT

- **Fortune 500 – Large Enterprise**
- 1200 locations in North America
- 65% Cost reduction with consolidation
- Deployed sites in 9 months with ZTP

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

ROLLINS

- **Global 1000 – Large Enterprise**
- 700 locations in 50 Countries
- 10X Improved user experience
- 50%+ reduced network set-up time

Fortinet won against

- *Cisco ISR Router*
- *VMWARE VeloCloud, Versa*

Petrol Ofisi

- **1800 locations in Europe**
- 50% reduction in MPLS cost
- 99% increased business continuity
- Expanded to SD-Branch

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

Global SD-WAN Customer Success Examples

- **Fortune 500 – Large Enterprise**
- 1200 locations in North America
- 65% Cost reduction with consolidation
- Deployed sites in 9 months with ZTP

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

- **Global 1000 – Large Enterprise**
- 700 locations in 50 Countries
- 10X Improved user experience
- 50%+ reduced network set-up time

Fortinet won against

- *Cisco ISR Router*
- *VMWARE VeloCloud, Versa*

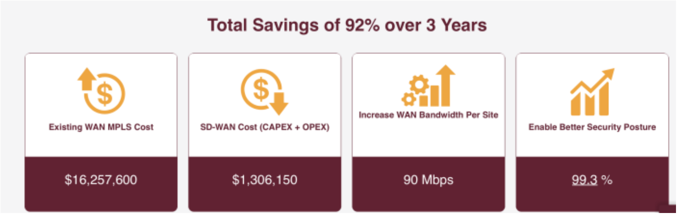
- **1800 locations in Europe**
- 50% reduction in MPLS cost
- 99% increased business continuity
- Expanded to SD-Branch

Fortinet won against

- *Cisco ISR Router*
- *Cisco Meraki*

SD-WAN Tools and Resources

ROI CALCULATOR



Total Savings of 92% over 3 Years

Existing WAN MPLS Cost	SD-WAN Cost (CAPEX + OPEX)	Increase WAN Bandwidth Per Site	Enable Better Security Posture
$16,257,600	$1,306,150	90 Mbps	99.3 %

Fortinet SD-WAN Real-World ROI Study

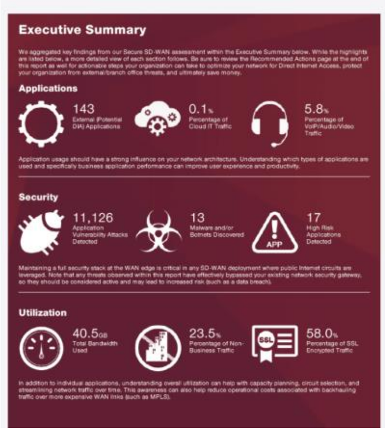
CUSTOMER WINS

Do the Right Thing. The Right Way.

Founded	202	$14B+	42K	21K	~1200
1971 Houston	Fortune 500 List	Annual Revenue	Employees	Trucks	Sites

30+ Global Customer Case studies

CTAP ASSESMENT



Executive Summary

We aggregated key findings from our Secure SD-WAN assessment within the Executive Summary below. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report as well for actionable steps your organization can take to optimize your network for Direct Internet Access, protect your organization from external/branch office threats, and ultimately save money.

Applications

143 External (Potential DIA) Applications

0.1% Percentage of Cloud IT Traffic

5.8% Percentage of VoIP/Audio/Video Traffic

Application usage should have a strong influence on your network architecture. Understanding which types of applications are used and specifically business application performance can improve user experience and productivity.

Security

11,126 Application Vulnerability Attacks Detected

13 Malware and/or Botnets Discovered

17 High Risk Applications Detected

Maintaining a full security stack at the WAN edge is critical in any SD-WAN deployment where public Internet circuits are leveraged. Note that any threats observed within this report have effectively bypassed your existing network security gateway, so they should be considered active and may lead to increased risk (such as a data breach).

Utilization

40.5GB Total Bandwidth Used

23.5% Percentage of Non-Business Traffic

58.0% Percentage of SSL Encrypted Traffic

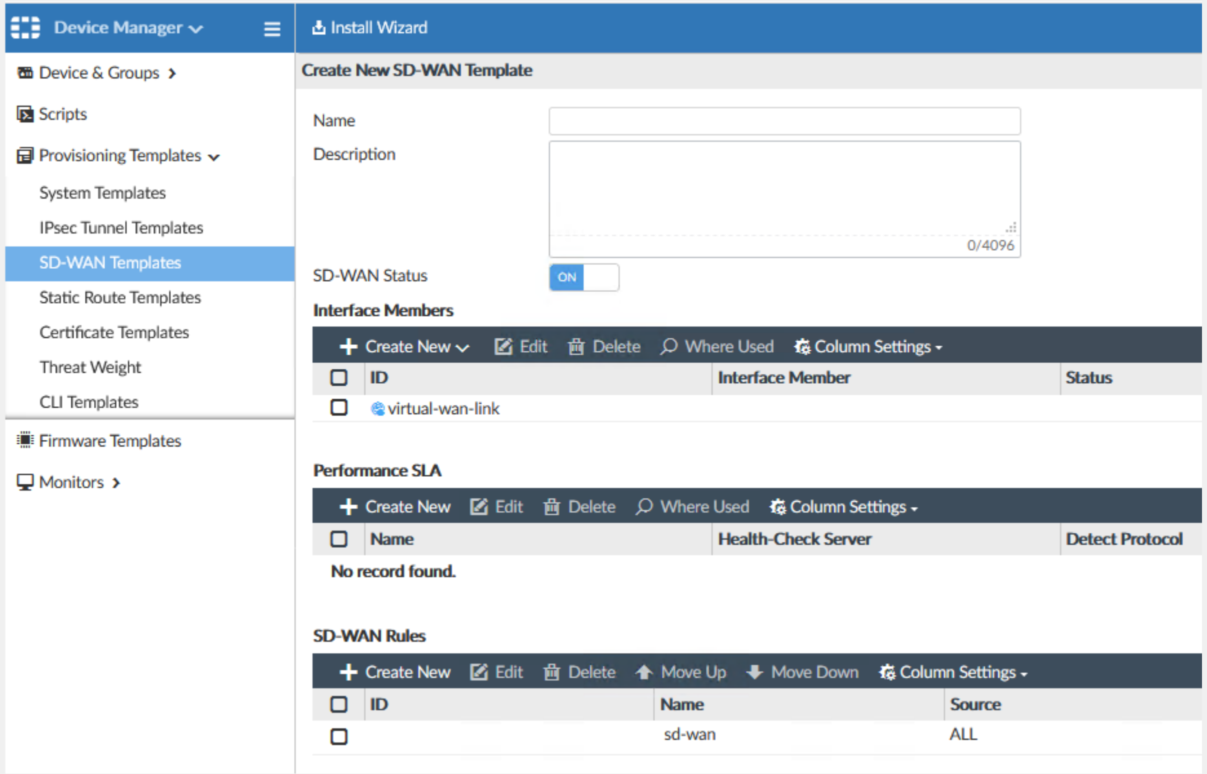
In addition to individual applications, understanding overall utilization can help with capacity planning, circuit selection, and streamlining network traffic over time. This awareness can also help reduce operational costs associated with backhauling traffic over more expensive WAN links (such as MPLS).

400+ customers completed SD-WAN Assessment

Configuring Secure SD-WAN

Configuring Secure SD-WAN

- Basic steps
  - Setup the VPNs
    - VPN Manager > IPsec VPN
  - Configure shared resources
    - Interface members
    - Health-check servers
    - BGP neighbors
    - Input interfaces
  - Create templates
  - Assign templates to devices



Create New SD-WAN Template

Name

Description 0/4096

SD-WAN Status ON

Interface Members

□	ID	Interface Member	Status
□	virtual-wan-link		

Performance SLA

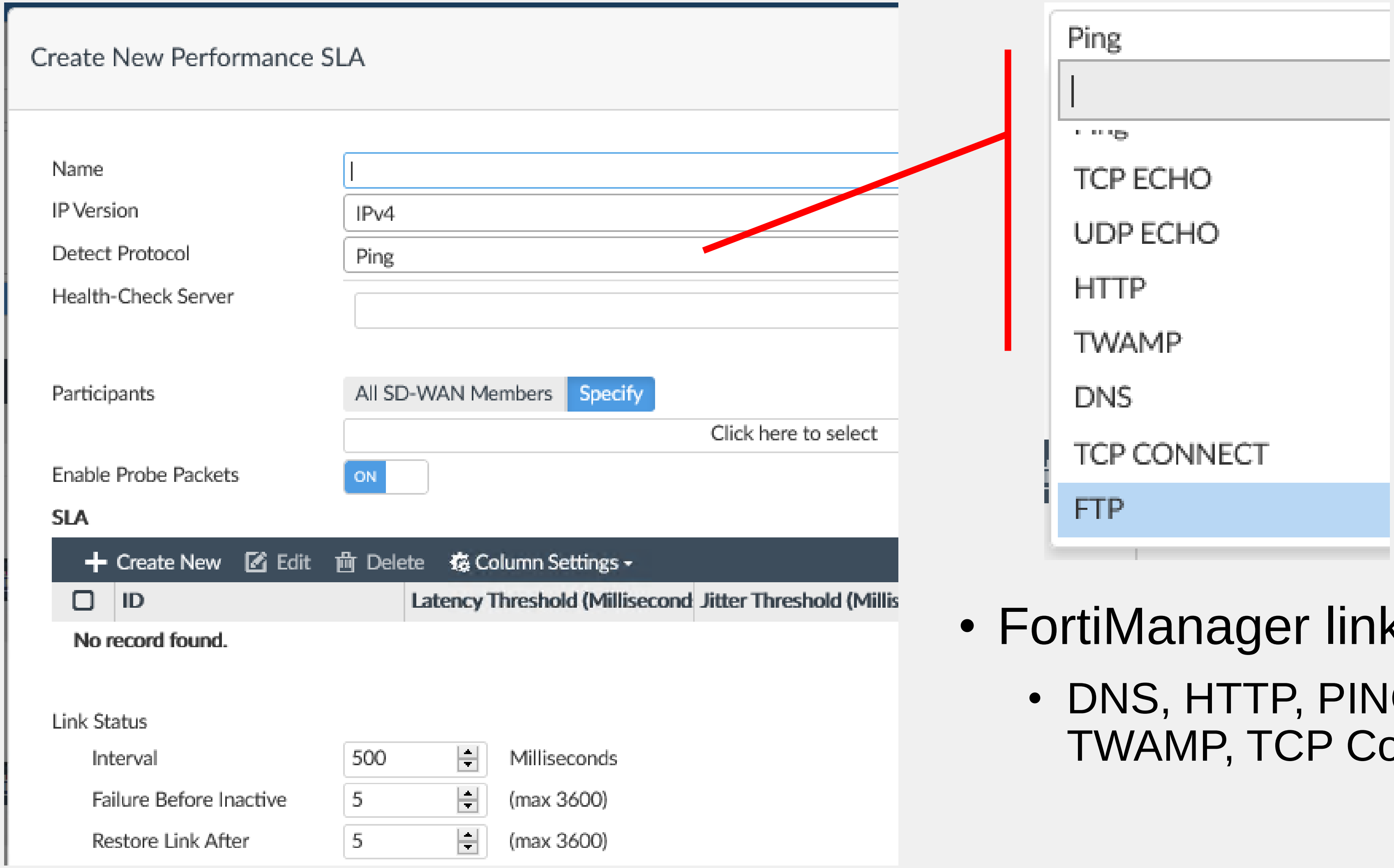
□	Name	Health-Check Server	Detect Protocol

No record found.

SD-WAN Rules

□	ID	Name	Source
□		sd-wan	ALL

Performance SLA—Link Health Monitor



Create New Performance SLA

Name	
IP Version	IPv4
Detect Protocol	Ping
Health-Check Server	
Participants	All SD-WAN Members / Specify
	Click here to select
Enable Probe Packets	ON

SLA

☐	ID	Latency Threshold (Millisecond	Jitter Threshold (Millis

No record found.

Link Status

Interval	500	Milliseconds
Failure Before Inactive	5	(max 3600)
Restore Link After	5	(max 3600)

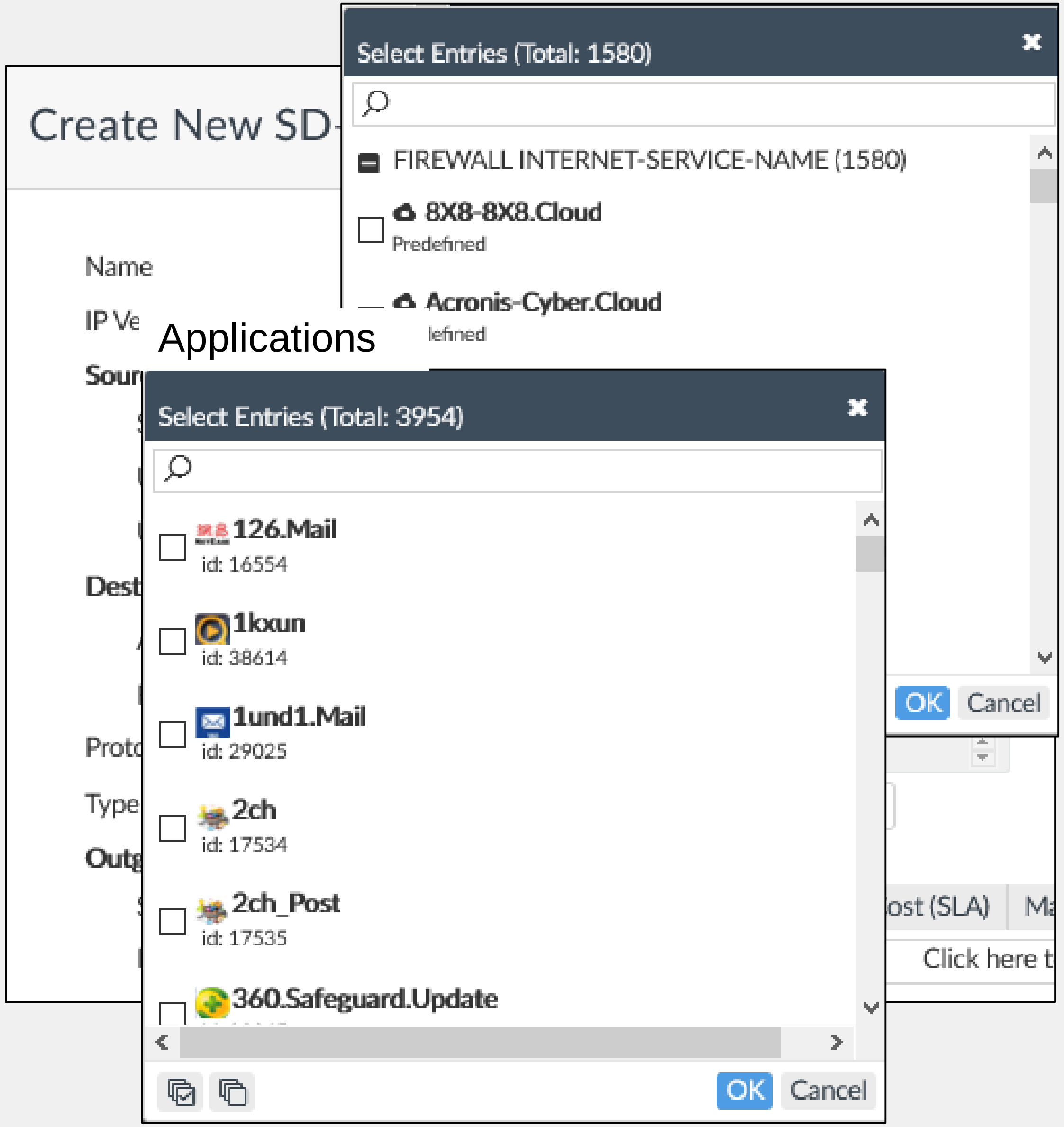
- FortiManager link health monitor options:
  - DNS, HTTP, PING, TCP echo, UDP echo, TWAMP, TCP Connect, and FTP

SD-WAN Rules

- Rules can match traffic based on:
  - Source IP address, destination IP address, or port number
  - Internet services database (ISDB) address object
  - Users or user groups
  - Type of service (ToS)

- Use rules to route traffic through the member interfaces that best fit your needs

- Rules can be created for specific Internet Services or Applications


Internet Services

Select Entries (Total: 1580)

FIREWALL INTERNET-SERVICE-NAME (1580)

□ 8X8-8X8.Cloud
Predefined

Acronis-Cyber.Cloud
lefined

Applications

Select Entries (Total: 3954)

□ 126.Mail
id: 16554

□ 1kxun
id: 38614

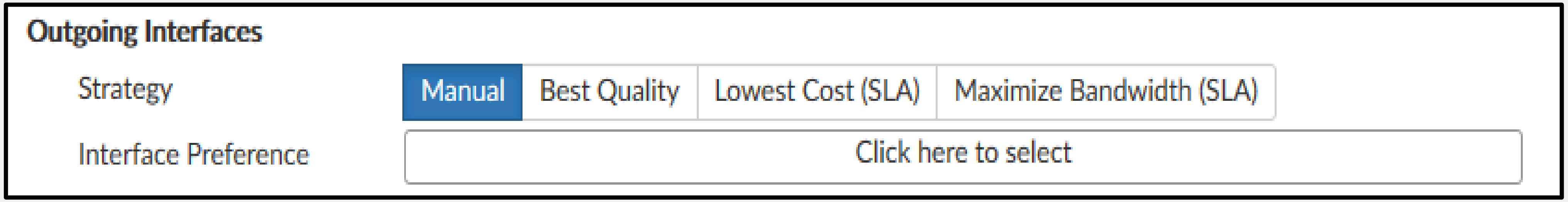
□ 1und1.Mail
id: 29025

□ 2ch
id: 17534

□ 2ch_Post
id: 17535

□ 360.Safeguard.Update

SD-WAN Rules—Manual



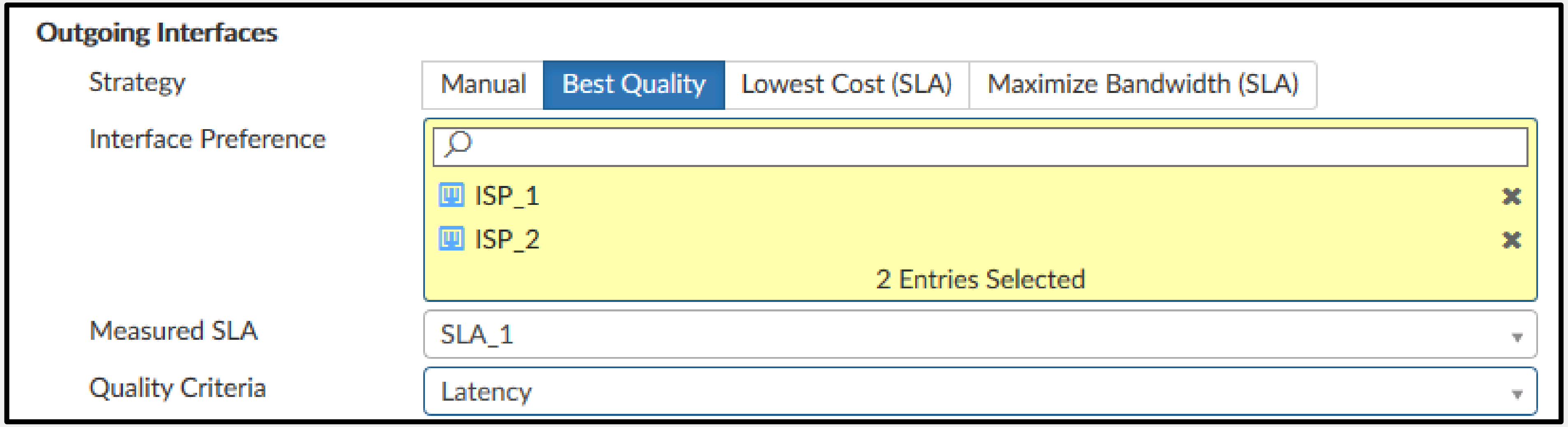
Outgoing Interfaces

Strategy: Manual | Best Quality | Lowest Cost (SLA) | Maximize Bandwidth (SLA) — Manual selected

Interface Preference: Click here to select

- Introduced in FortiOS 6.2
- Use a manual rule to pin one or more applications to a specific SD-WAN member interface

SD-WAN Rules—Best Quality



Outgoing Interfaces

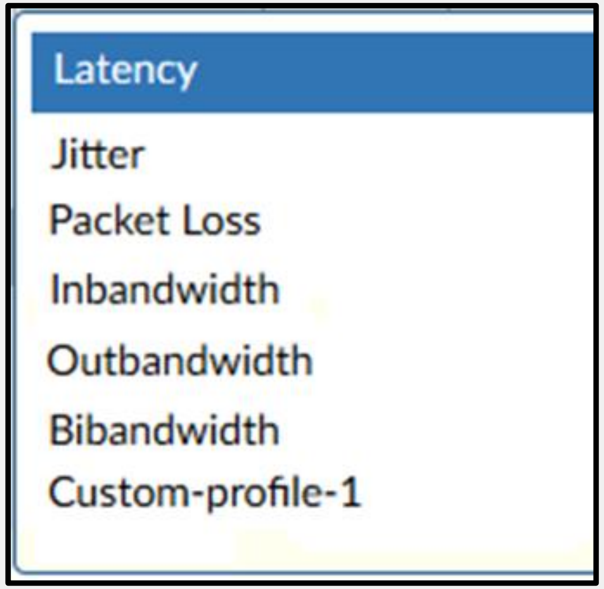
Strategy: Best Quality

Interface Preference: ISP_1, ISP_2

2 Entries Selected

Measured SLA: SLA_1

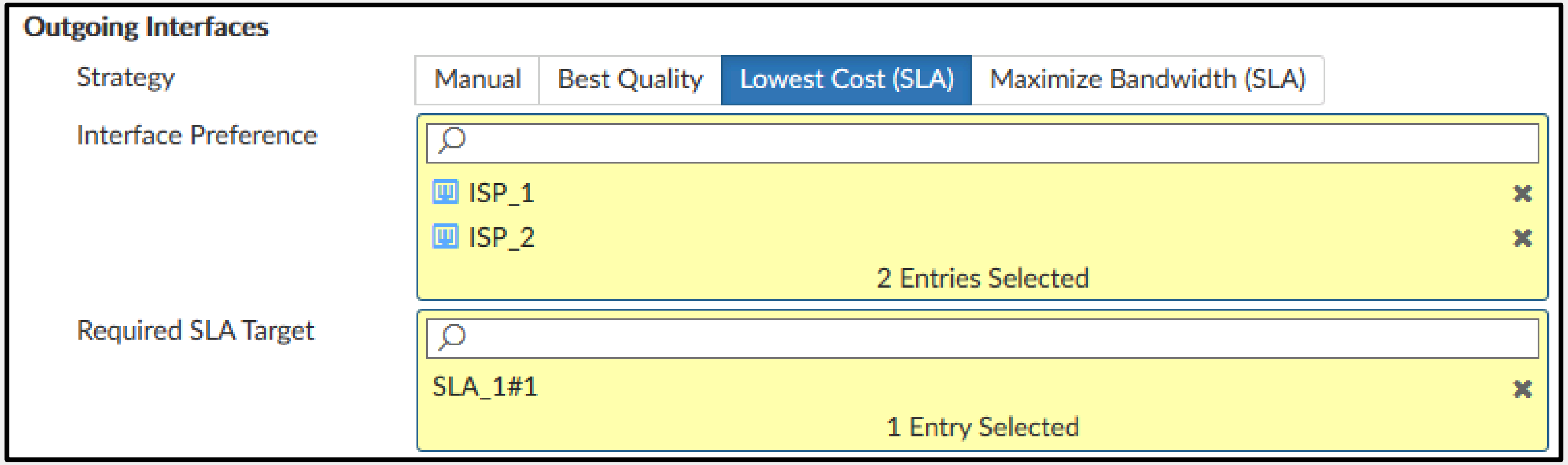
Quality Criteria: Latency



Custom-Profile-1

Link quality = (a*latency)+(b*jitter)+(c*packet loss)+(d/bandwidth)

SD-WAN Rules—Lowest Cost (SLA)



Outgoing Interfaces

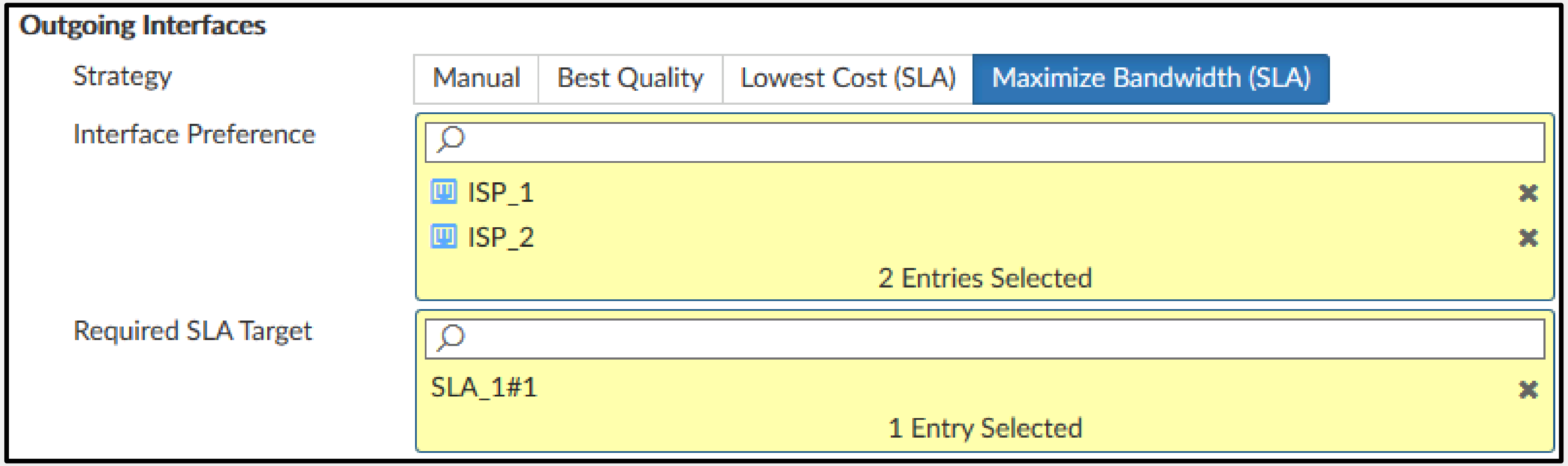
Strategy: Manual | Best Quality | Lowest Cost (SLA) | Maximize Bandwidth (SLA)

Interface Preference: ISP_1, ISP_2 — 2 Entries Selected

Required SLA Target: SLA_1#1 — 1 Entry Selected

- All of the traffic that matches the rule will be directed to a single interface
- Uses the cost value of the SD-WAN member interface

SD-WAN Rules—Maximize Bandwidth (SLA)



Outgoing Interfaces

Strategy: Manual | Best Quality | Lowest Cost (SLA) | Maximize Bandwidth (SLA)

Interface Preference: ISP_1, ISP_2 — 2 Entries Selected

Required SLA Target: SLA_1#1 — 1 Entry Selected

- Introduced in FortiOS 6.2
- Load balances multiple sessions across participating SD-WAN members that meet the SLA

Conclusions:

- Customers want WAN with local internet breakout
  - SD-WAN enables local internet breakout but this means added security risks
  - Most SD-WAN vendors do not have robust NGFW security
    - Many SD-WAN vendors recommend multiple devices for SD-WAN and security
    - Multiple devices add to the complexity and cost
- What customers need is Secure SD-WAN
  - A single device handles both the security and the SD-WAN needs

Key Takeaway

- FortiGate changes the conversation from SD-WAN to Secure SD-WAN
  - Best of breed integrated SD-WAN networking and security capabilities in a single device reduces TCO
- FortiGate is SD-WAN ready:
  - Purpose-built security processor (ASIC) for high reliability
  - Enhanced application aware WAN path controller for QoS
  - Security Fabric ready for easy visibility and control
  - FortiManager enables single pane management across thousands of enterprise branches
  - 360 Protection is the most comprehensive protection bundle

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:

- **Ask your instructor for a course completion certificate**
- **Course Name:** Constructing a Secure SD-WAN Architecture
- **Number of training hours:** 4 hours
- **(ISC)^2 CISSP Domain 4:** Communication and Network Security
- Provide the **date** you completed the training

FORTINET
NSE Training Institute

(ISC)$^{2®}$
CPE SUBMITTER

Fortinet provides ILT Training

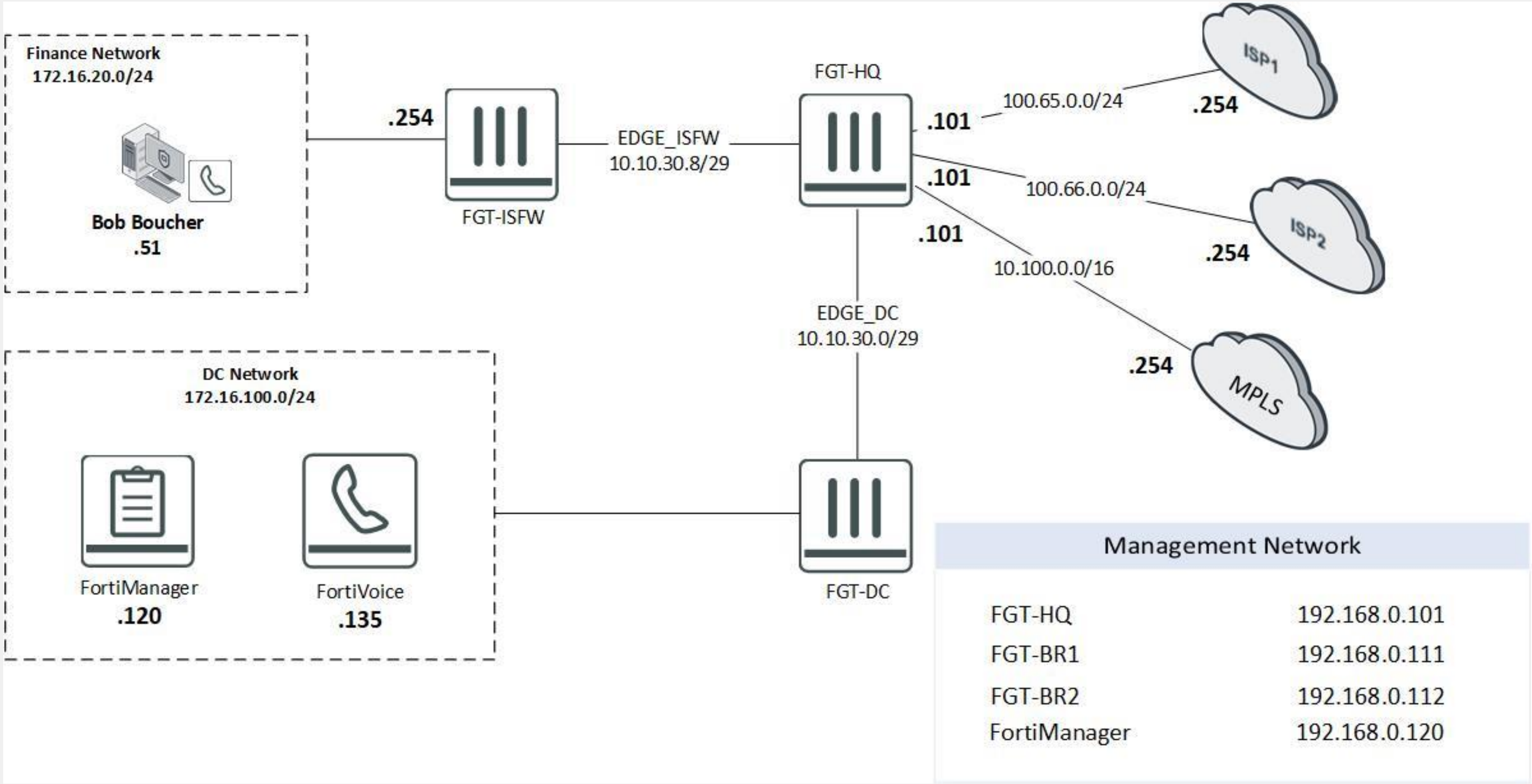
Log into https://training.fortinet.com to find out more:

- **A full range of Instructor led, product based training courses leading to certification, based on lectures and labs.**
- **Free Cybersecurity Training**
  - **Advanced training** for security professionals.
    Technical training for IT professionals.
    Awareness training for teleworkers.

FORTINET
NSE Training Institute

Lab Exercise: SD-WAN

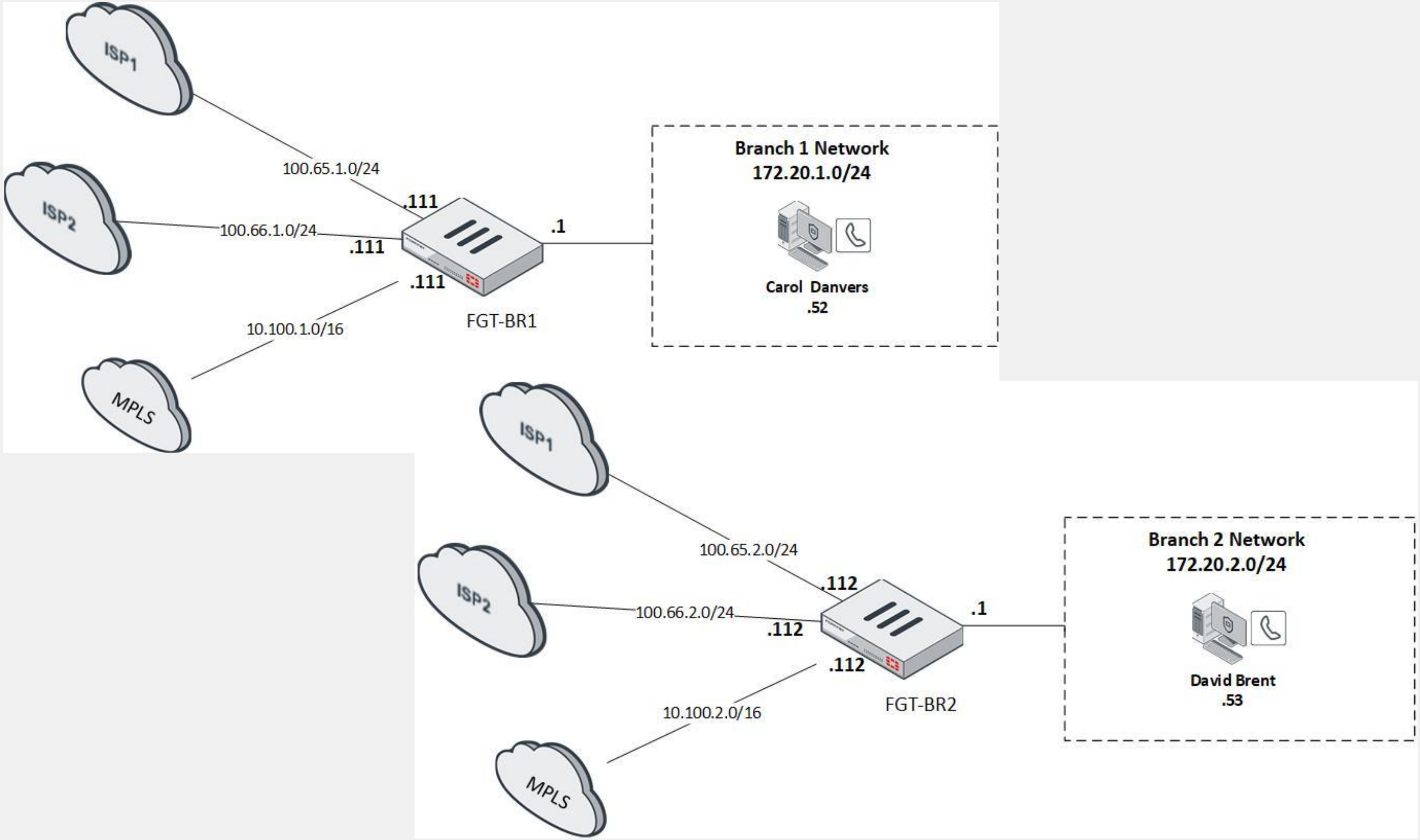
Lab—Network Diagram



Management Network

FGT-HQ	192.168.0.101
FGT-BR1	192.168.0.111
FGT-BR2	192.168.0.112
FortiManager	192.168.0.120

Lab—Network Diagram



Instructor Notes

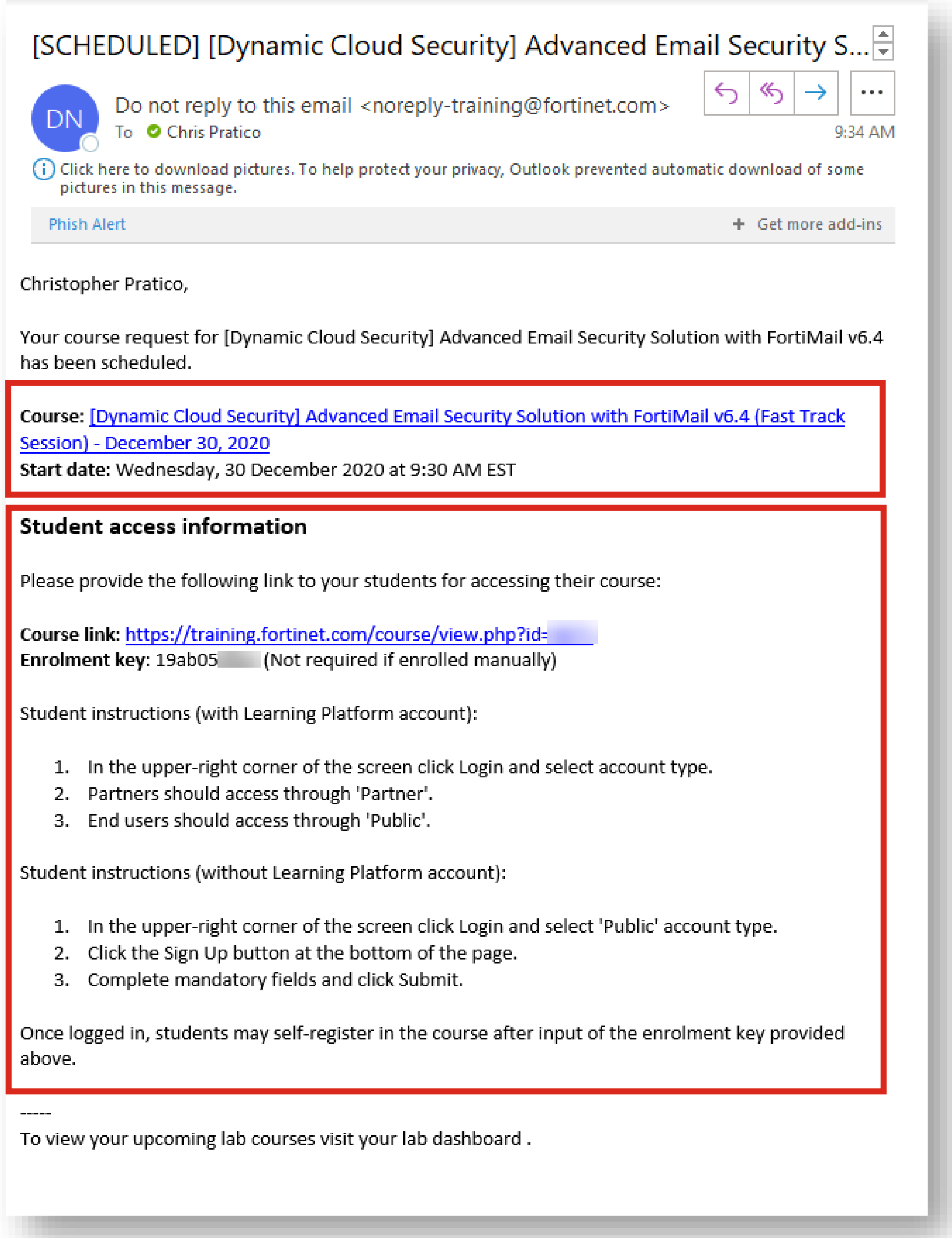
Instructor Notes

- The following slides are informational and can be used for the following:
  - To remind instructors how to interact with the Fast Track labs
  - To help students get started using the hands-on lab
- Feel free to use some, all, or none of the slides as part of your session
- The interfaces should be fairly intuitive; therefore, it is recommended to keep the initial instruction short and then assist students individually as needed

Student Access

- The student course link and enrolment key is provided via email after the session has been approved

- Instructions for access can be forwarded to students



[SCHEDULED] [Dynamic Cloud Security] Advanced Email Security S...
DN
Do not reply to this email <noreply-training@fortinet.com>
To ✔ Chris Pratico
9:34 AM
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
Phish Alert
+ Get more add-ins

Christopher Pratico,

Your course request for [Dynamic Cloud Security] Advanced Email Security Solution with FortiMail v6.4 has been scheduled.

Course: [Dynamic Cloud Security] Advanced Email Security Solution with FortiMail v6.4 (Fast Track Session) - December 30, 2020
Start date: Wednesday, 30 December 2020 at 9:30 AM EST

Student access information

Please provide the following link to your students for accessing their course:

Course link: https://training.fortinet.com/course/view.php?id=[redacted]
Enrolment key: 19ab05[redacted] (Not required if enrolled manually)

Student instructions (with Learning Platform account):

1. In the upper-right corner of the screen click Login and select account type.
2. Partners should access through 'Partner'.
3. End users should access through 'Public'.

Student instructions (without Learning Platform account):

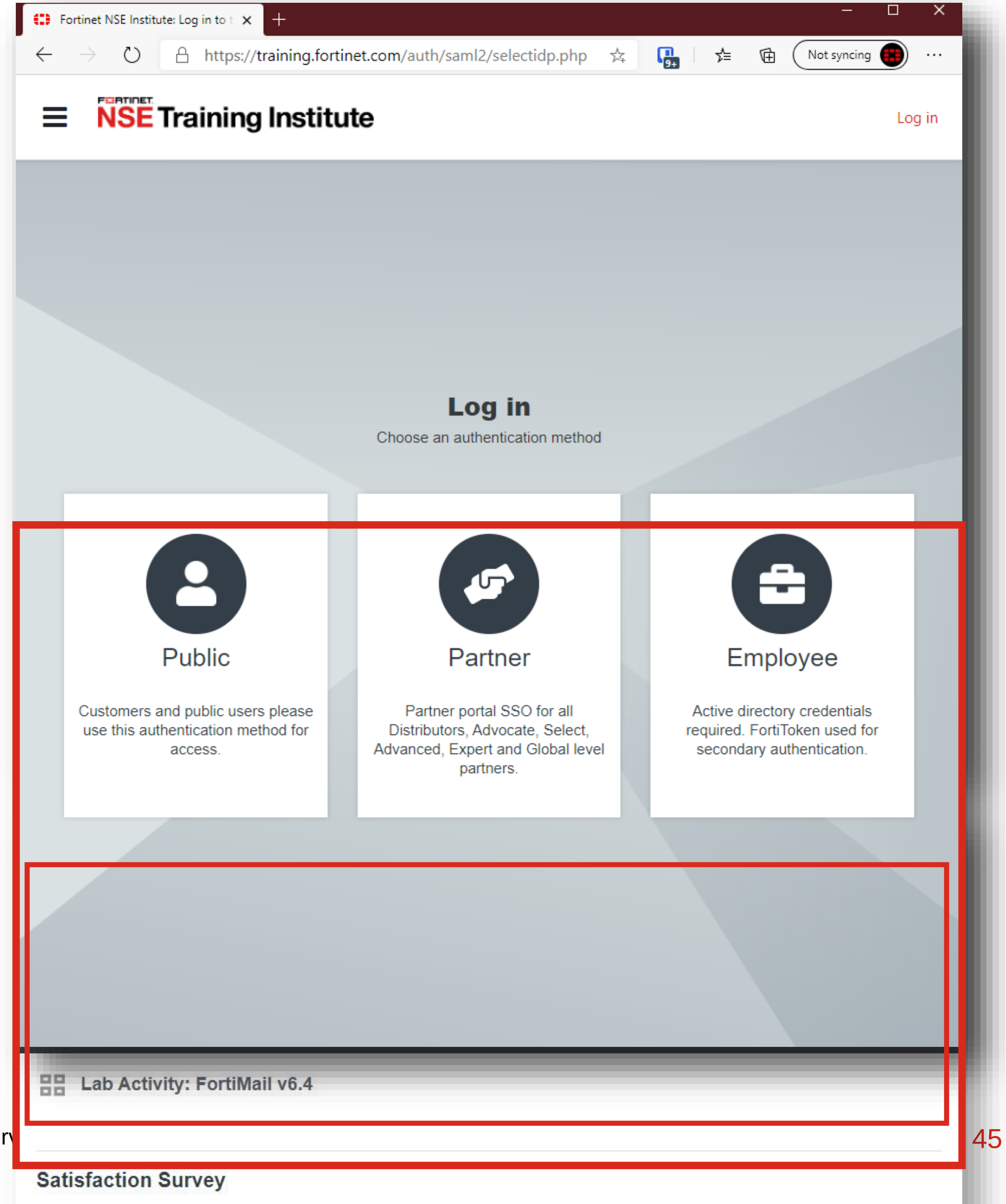
1. In the upper-right corner of the screen click Login and select 'Public' account type.
2. Click the Sign Up button at the bottom of the page.
3. Complete mandatory fields and click Submit.

Once logged in, students may self-register in the course after input of the enrolment key provided above.

To view your upcoming lab courses visit your lab dashboard .

Fast Track Course

- Log in via the appropriate authentication method
- Enter the provided enrolment key
- The hands-on Lab accessible from **Lab Activity** link
- Course content is available for download after completing the hands-on lab and short survey



Fortinet NSE Institute: Log in to t

https://training.fortinet.com/auth/saml2/selectidp.php

Not syncing

FORTINET NSE Training Institute

Log in

Log in

Choose an authentication method

Public

Customers and public users please use this authentication method for access.

Partner

Partner portal SSO for all Distributors, Advocate, Select, Advanced, Expert and Global level partners.

Employee

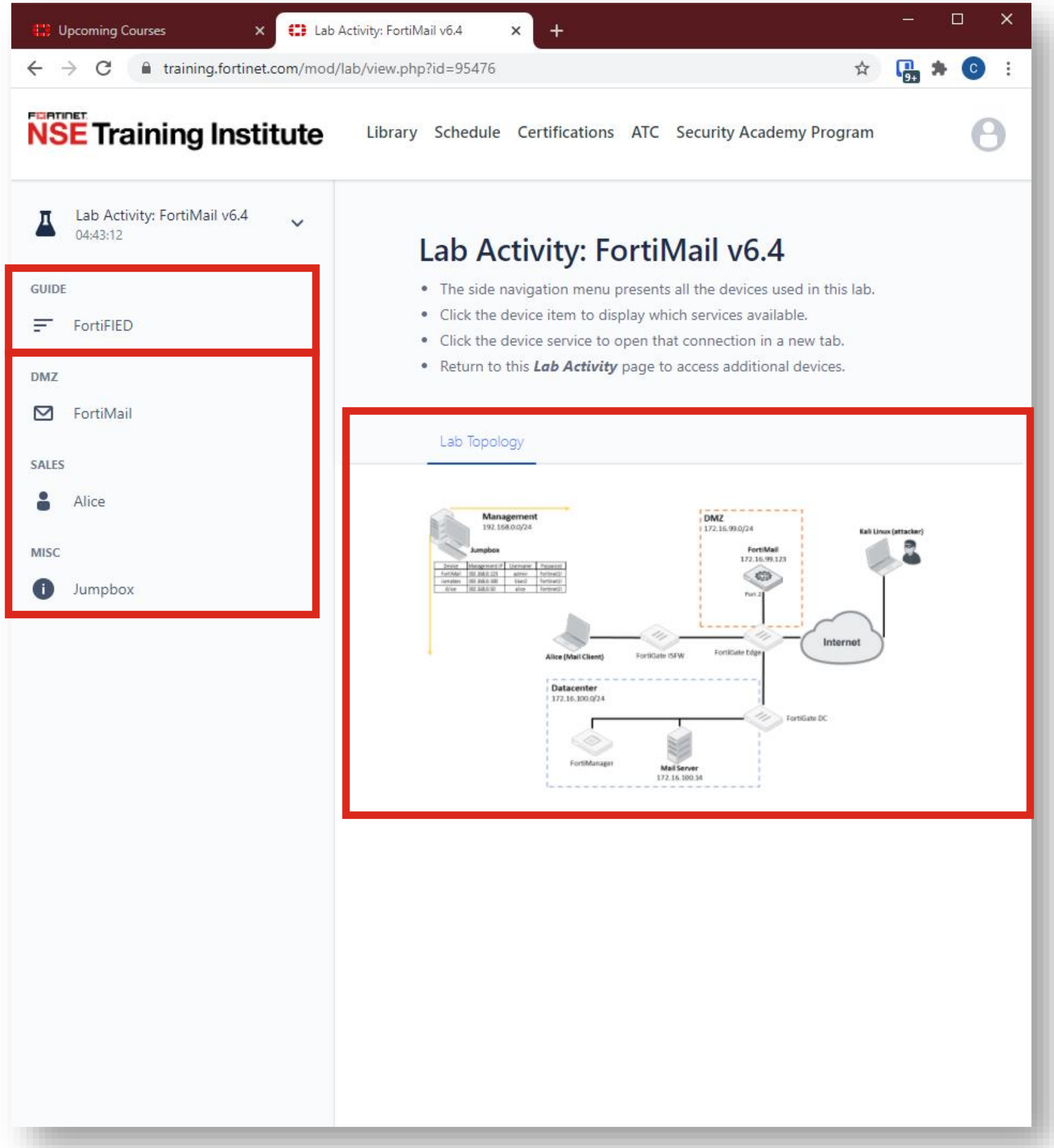
Active directory credentials required. FortiToken used for secondary authentication.

Lab Activity: FortiMail v6.4

Satisfaction Survey

Lab Activity

- Students individual hands-on lab environment
- Reference lab topology
- Online **FortiFIED** lab guide
- Direct access to lab devices



Lab Activity: FortiMail v6.4

- The side navigation menu presents all the devices used in this lab.
- Click the device item to display which services available.
- Click the device service to open that connection in a new tab.
- Return to this ***Lab Activity*** page to access additional devices.

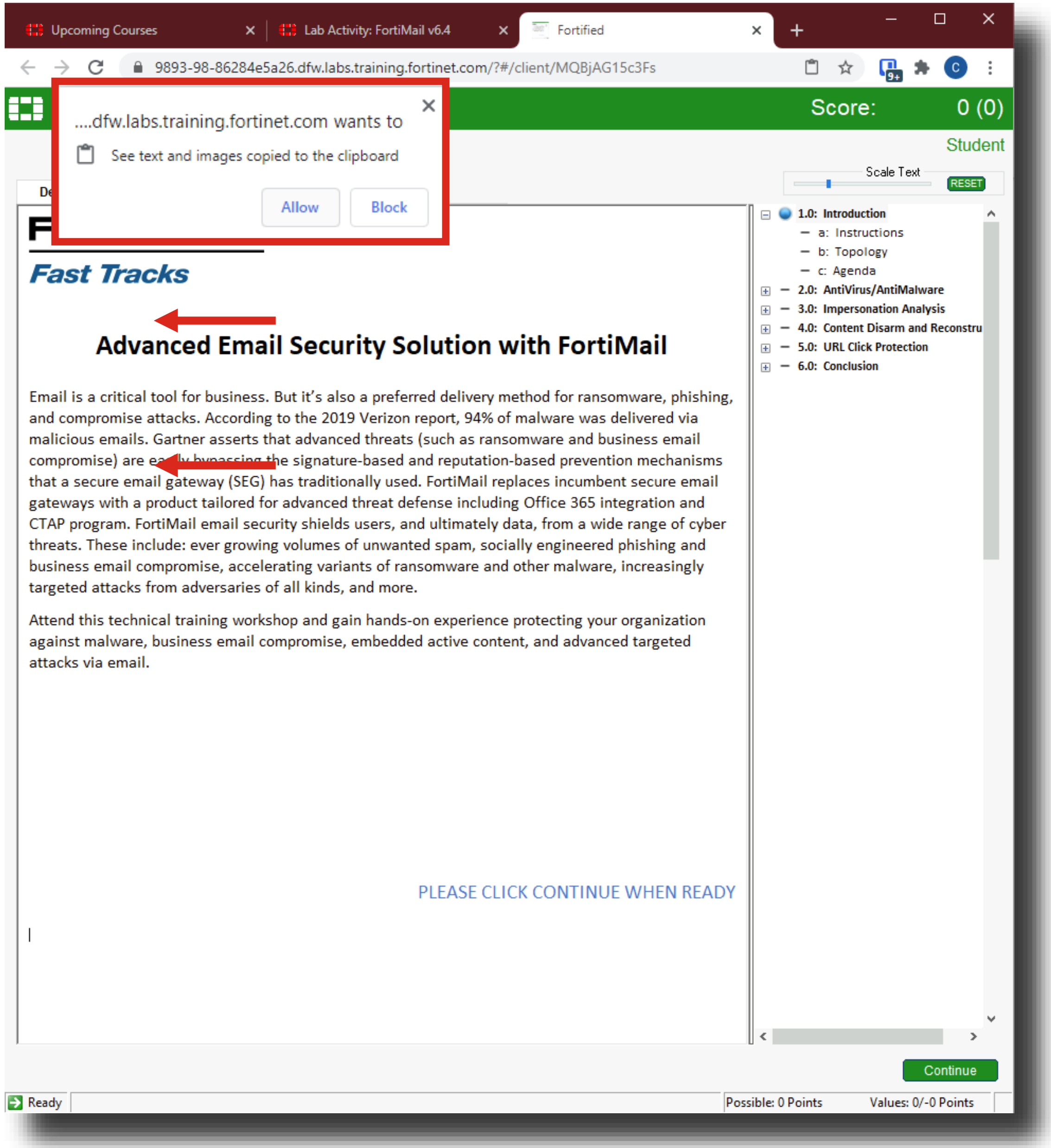
Device	Management IP	Username	Password
FortiMail	192.168.0.123	admin	fortinet1!
[illegible]	192.168.0.100	[illegible]	fortinet1!
Alice	192.168.0.50	alice	fortinet1!

FortiFIED Lab Guide Access

1. From the **Lab Activity** page click **FortFIED** on the navigation sidebar.

2. Click the **RDP** connection to open a new tab containing the lab guide.

3. If displayed, allow the browser to copy/paste tab contents to the clipboard.



....dfw.labs.training.fortinet.com wants to

See text and images copied to the clipboard

1.0: Introduction
- a: Instructions
- b: Topology
- c: Agenda
- 2.0: AntiVirus/AntiMalware
- 3.0: Impersonation Analysis
- 4.0: Content Disarm and Reconstru
- 5.0: URL Click Protection
- 6.0: Conclusion

Fast Tracks

Advanced Email Security Solution with FortiMail

Email is a critical tool for business. But it's also a preferred delivery method for ransomware, phishing, and compromise attacks. According to the 2019 Verizon report, 94% of malware was delivered via malicious emails. Gartner asserts that advanced threats (such as ransomware and business email compromise) are easily bypassing the signature-based and reputation-based prevention mechanisms that a secure email gateway (SEG) has traditionally used. FortiMail replaces incumbent secure email gateways with a product tailored for advanced threat defense including Office 365 integration and CTAP program. FortiMail email security shields users, and ultimately data, from a wide range of cyber threats. These include: ever growing volumes of unwanted spam, socially engineered phishing and business email compromise, accelerating variants of ransomware and other malware, increasingly targeted attacks from adversaries of all kinds, and more.

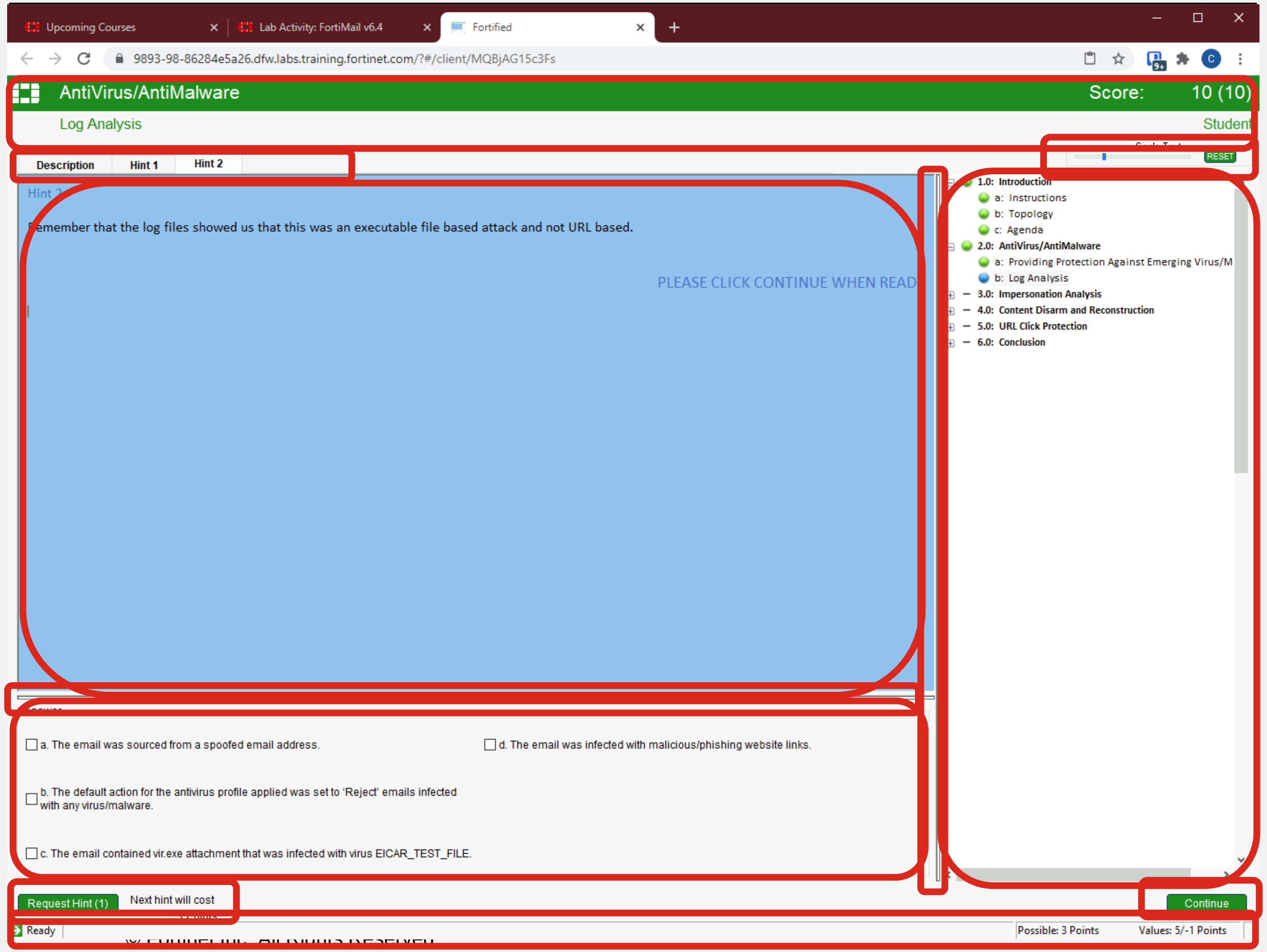
Attend this technical training workshop and gain hands-on experience protecting your organization against malware, business email compromise, embedded active content, and advanced targeted attacks via email.

PLEASE CLICK CONTINUE WHEN READY

FortiFIED Interactive Lab Guide

Stop and Think Objective

- Enter a name
- Application banner
- Objectives list
- Display tabs
- Rich text
- Answer choice
- Continue button
- Status bar
- Scale text slider
- Resize display bar
- Hints



Remember that the log files showed us that this was an executable file based attack and not URL based.

PLEASE CLICK CONTINUE WHEN READ

- 1.0: Introduction
  - a: Instructions
  - b: Topology
  - c: Agenda
- 2.0: AntiVirus/AntiMalware
  - a: Providing Protection Against Emerging Virus/M
  - b: Log Analysis
- 3.0: Impersonation Analysis
- 4.0: Content Disarm and Reconstruction
- 5.0: URL Click Protection
- 6.0: Conclusion

□ a. The email was sourced from a spoofed email address.

□ b. The default action for the antivirus profile applied was set to 'Reject' emails infected with any virus/malware.

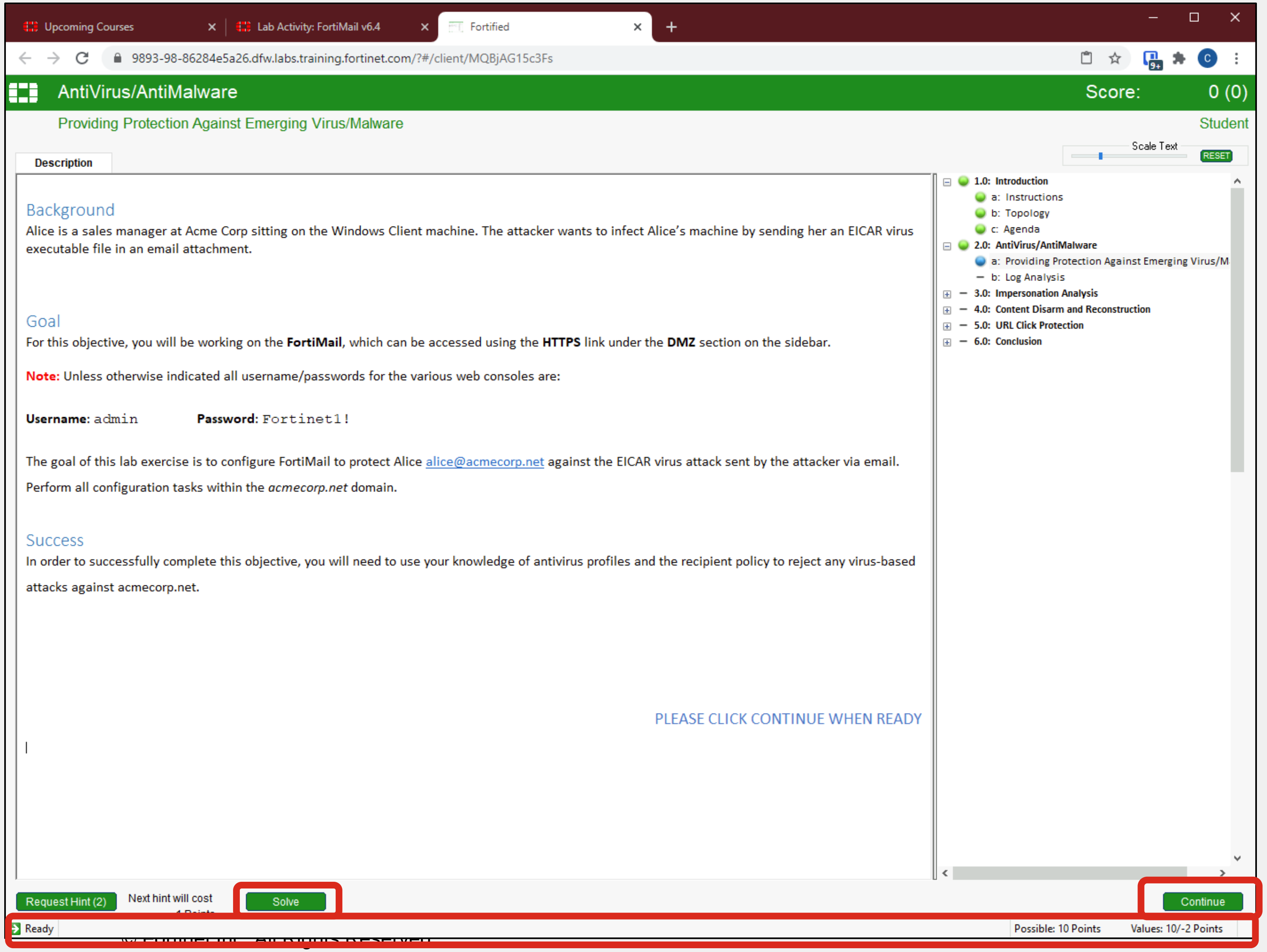
□ c. The email contained vir.exe attachment that was infected with virus EICAR_TEST_FILE.

□ d. The email was infected with malicious/phishing website links.

FortiFIED Interactive Lab Guide

Task Objective

- Task success is determined by script after clicking **Continue**
- Success or Failure will be indicated on the **status bar**
- **Solve** may be available on some objectives (use with caution)


Upcoming Courses
Lab Activity: FortiMail v6.4
Fortified
9893-98-86284e5a26.dfw.labs.training.fortinet.com/?#/client/MQBjAG15c3Fs
AntiVirus/AntiMalware
Score: 0 (0)
Providing Protection Against Emerging Virus/Malware
Student
Scale Text
RESET
Description
1.0: Introduction
a: Instructions
b: Topology
c: Agenda
2.0: AntiVirus/AntiMalware
a: Providing Protection Against Emerging Virus/M
b: Log Analysis
3.0: Impersonation Analysis
4.0: Content Disarm and Reconstruction
5.0: URL Click Protection
6.0: Conclusion
Request Hint (2)
Next hint will cost
Solve
Continue
Ready
Possible: 10 Points
Values: 10/-2 Points

Background

Alice is a sales manager at Acme Corp sitting on the Windows Client machine. The attacker wants to infect Alice's machine by sending her an EICAR virus executable file in an email attachment.

Goal

For this objective, you will be working on the **FortiMail**, which can be accessed using the **HTTPS** link under the **DMZ** section on the sidebar.

Note: Unless otherwise indicated all username/passwords for the various web consoles are:

Username: `admin` **Password:** `Fortinet1!`

The goal of this lab exercise is to configure FortiMail to protect Alice alice@acmecorp.net against the EICAR virus attack sent by the attacker via email.

Perform all configuration tasks within the *acmecorp.net* domain.

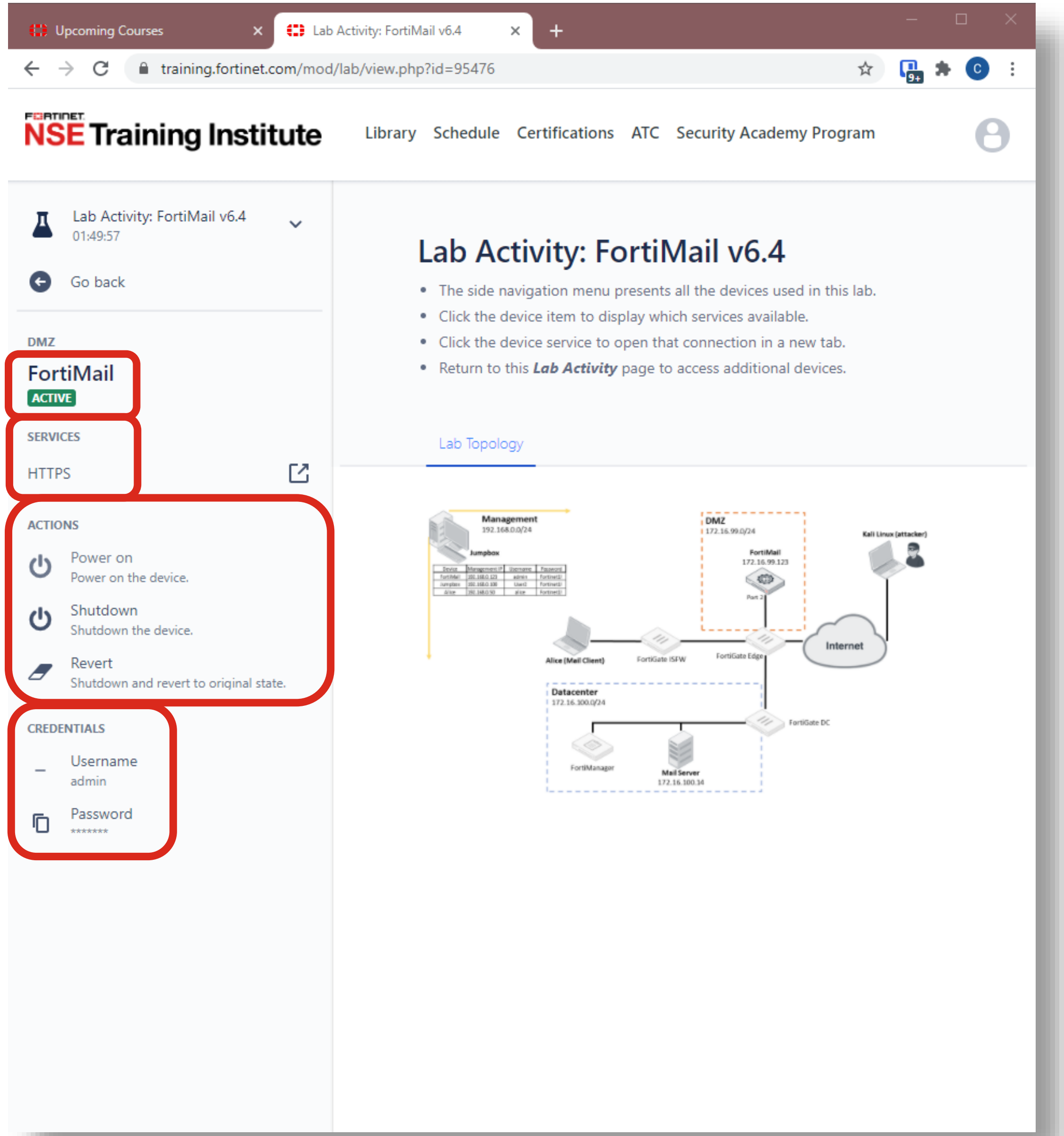
Success

In order to successfully complete this objective, you will need to use your knowledge of antivirus profiles and the recipient policy to reject any virus-based attacks against acmecorp.net.

PLEASE CLICK CONTINUE WHEN READY

Device Access

- Status
  - Active / Inactive / Unknown
- Services
  - RDP / HTTPS / SSH
  - Click to open in a new tab
- Actions
  - Power on / Shutdown / Revert
- Credentials
  - Click to copy to clipboard



Upcoming Courses ✕ | Lab Activity: FortiMail v6.4 ✕ | +

training.fortinet.com/mod/lab/view.php?id=95476

FORTINET NSE Training Institute — Library | Schedule | Certifications | ATC | Security Academy Program

Lab Activity: FortiMail v6.4
01:49:57

Go back

DMZ

FortiMail
ACTIVE

SERVICES

HTTPS

ACTIONS

Power on
Power on the device.

Shutdown
Shutdown the device.

Revert
Shutdown and revert to original state.

CREDENTIALS

Username
admin

Password
****

Lab Activity: FortiMail v6.4

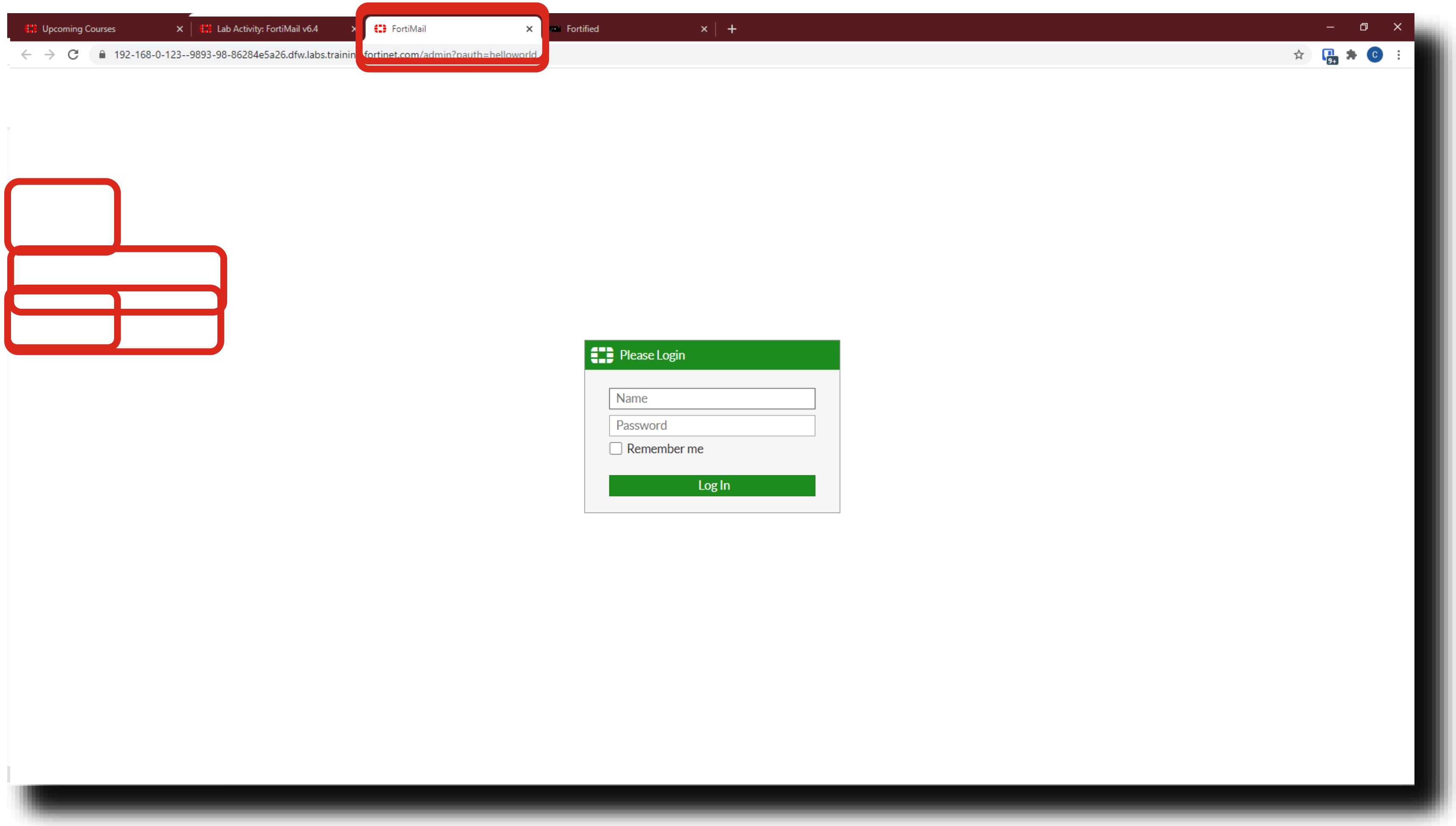
- The side navigation menu presents all the devices used in this lab.
- Click the device item to display which services available.
- Click the device service to open that connection in a new tab.
- Return to this ***Lab Activity*** page to access additional devices.

Lab Topology

Device	Management IP	Username	Password
FortiMail	192.168.0.123	admin	Fortinet1!
Jumpbox	192.168.0.100	User1	Fortinet1!
Alice	192.168.0.50	alice	Fortinet1!

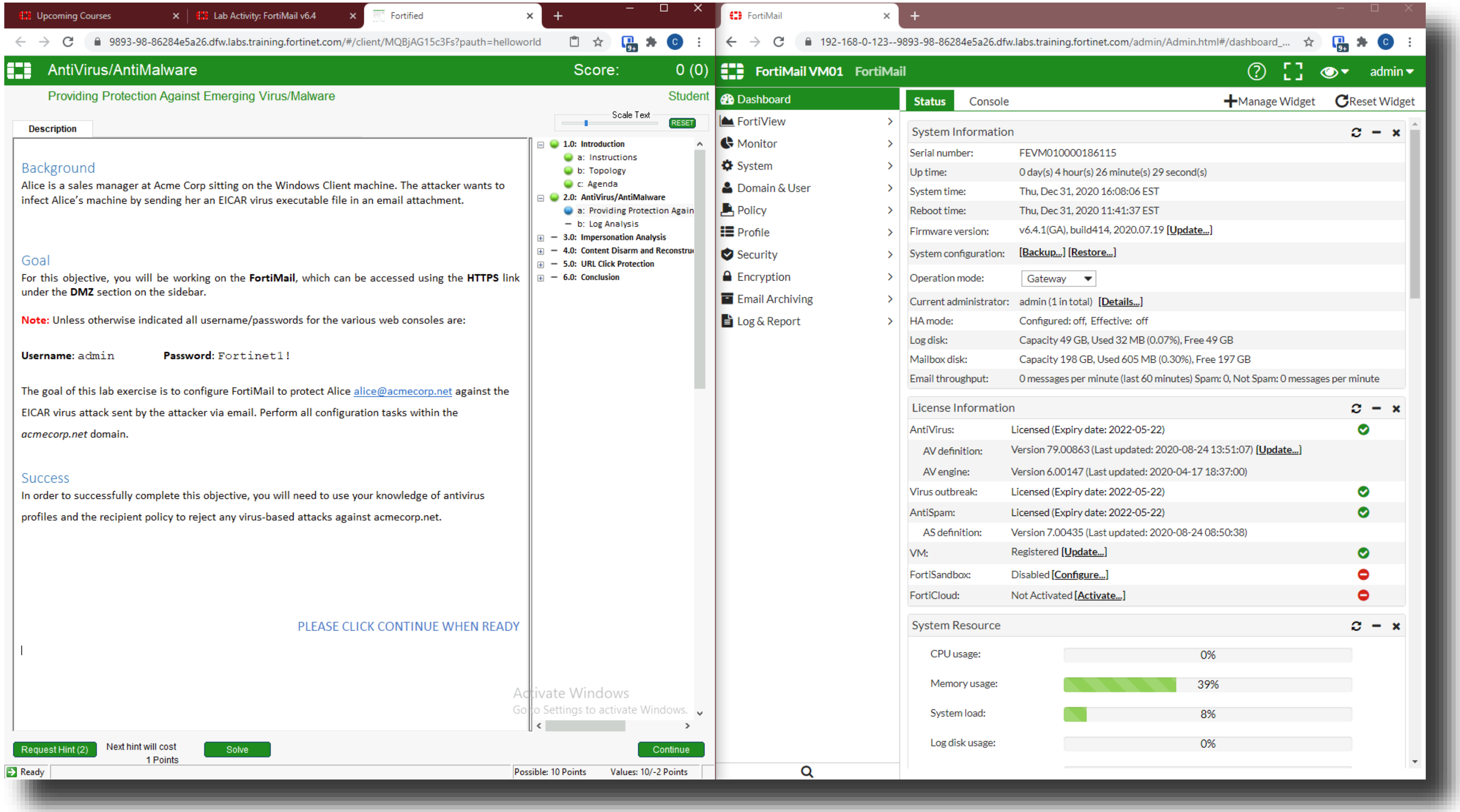
Window Adjustments

- Access the FortiFIED lab guide
- Access any other device


Upcoming Courses
Lab Activity: FortiMail v6.4
FortiMail
Fortified
192-168-0-123--9893-98-86284e5a26.dfw.labs.traininfortinet.com/admin?pauth=helloworld
Please Login
Name
Password
□ Remember me
Log In

Window Adjustments for Single Monitors

- Drag tab from browser to separate
- Place windows side-by-side according to personal preference
- Complete hands-on lab


Upcoming Courses
Lab Activity: FortiMail v6.4
Fortified
9893-98-86284e5a26.dfw.labs.training.fortinet.com/#/client/MQBjAG15c3Fs?pauth=helloworld
AntiVirus/AntiMalware
Score: 0 (0)
Providing Protection Against Emerging Virus/Malware
Student
Description
Scale Text
RESET
1.0: Introduction
a: Instructions
b: Topology
c: Agenda
2.0: AntiVirus/AntiMalware
a: Providing Protection Again
b: Log Analysis
3.0: Impersonation Analysis
4.0: Content Disarm and Reconstru
5.0: URL Click Protection
6.0: Conclusion
Activate Windows
Go to Settings to activate Windows.
Request Hint (2)
Next hint will cost 1 Points
Solve
Continue
Ready
Possible: 10 Points
Values: 10/-2 Points
FortiMail
192-168-0-123--9893-98-86284e5a26.dfw.labs.training.fortinet.com/admin/Admin.html#/dashboard_...
FortiMail VM01 FortiMail
admin
Dashboard
FortiView
Monitor
System
Domain & User
Policy
Profile
Security
Encryption
Email Archiving
Log & Report
Status
Console
Manage Widget
Reset Widget

Background

Alice is a sales manager at Acme Corp sitting on the Windows Client machine. The attacker wants to infect Alice's machine by sending her an EICAR virus executable file in an email attachment.

Goal

For this objective, you will be working on the **FortiMail**, which can be accessed using the **HTTPS** link under the **DMZ** section on the sidebar.

Note: Unless otherwise indicated all username/passwords for the various web consoles are:

Username: `admin` **Password:** `Fortinet1!`

The goal of this lab exercise is to configure FortiMail to protect Alice alice@acmecorp.net against the EICAR virus attack sent by the attacker via email. Perform all configuration tasks within the *acmecorp.net* domain.

Success

In order to successfully complete this objective, you will need to use your knowledge of antivirus profiles and the recipient policy to reject any virus-based attacks against acmecorp.net.

PLEASE CLICK CONTINUE WHEN READY

System Information

Serial number:	FEVM010000186115
Up time:	0 day(s) 4 hour(s) 26 minute(s) 29 second(s)
System time:	Thu, Dec 31, 2020 16:08:06 EST
Reboot time:	Thu, Dec 31, 2020 11:41:37 EST
Firmware version:	v6.4.1(GA), build414, 2020.07.19 [Update...]
System configuration:	[Backup...] [Restore...]
Operation mode:	Gateway
Current administrator:	admin (1 in total) [Details...]
HA mode:	Configured: off, Effective: off
Log disk:	Capacity 49 GB, Used 32 MB (0.07%), Free 49 GB
Mailbox disk:	Capacity 198 GB, Used 605 MB (0.30%), Free 197 GB
Email throughput:	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

License Information

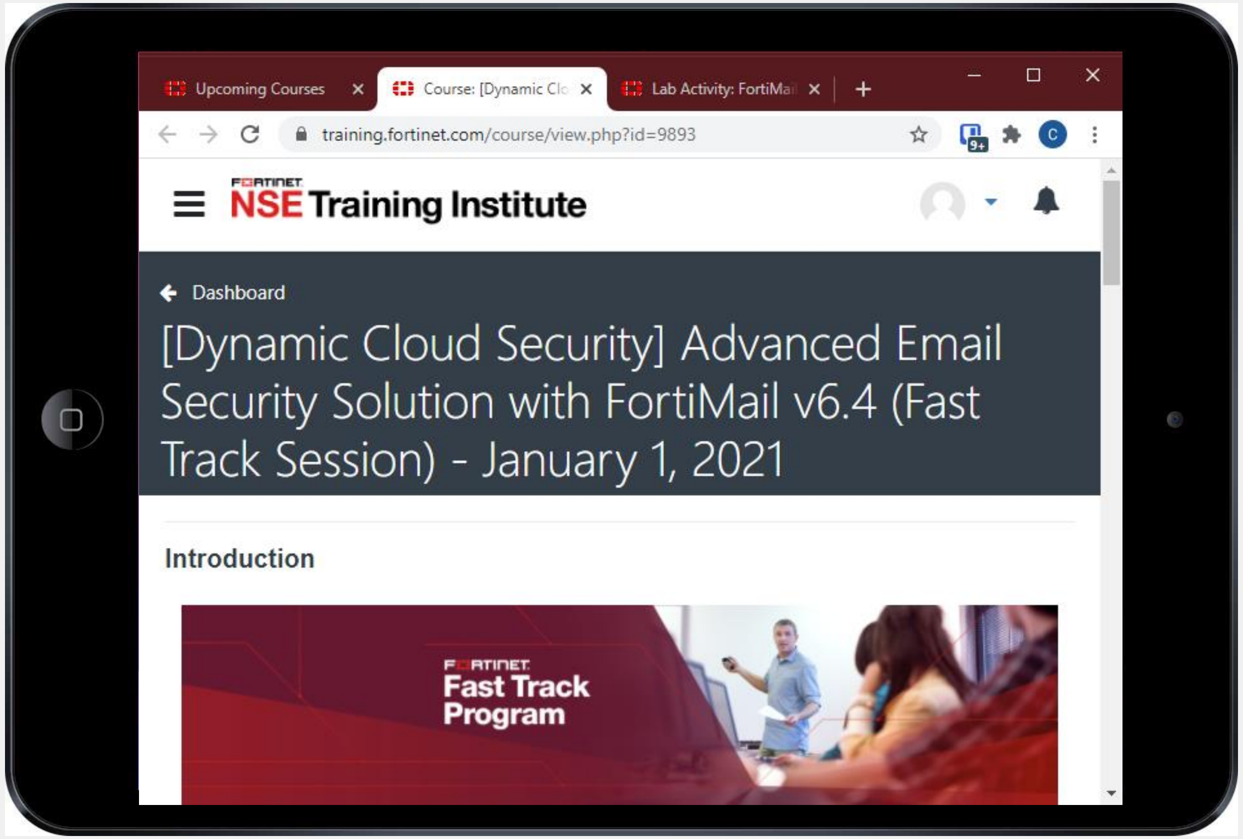
AntiVirus:	Licensed (Expiry date: 2022-05-22)	✓
AV definition:	Version 79.00863 (Last updated: 2020-08-24 13:51:07) [Update...]	
AV engine:	Version 6.00147 (Last updated: 2020-04-17 18:37:00)	
Virus outbreak:	Licensed (Expiry date: 2022-05-22)	✓
AntiSpam:	Licensed (Expiry date: 2022-05-22)	✓
AS definition:	Version 7.00435 (Last updated: 2020-08-24 08:50:38)	
VM:	Registered [Update...]	✓
FortiSandbox:	Disabled [Configure...]	⛔
FortiCloud:	Not Activated [Activate...]	⛔

System Resource

CPU usage:	0%
Memory usage:	39%
System load:	8%
Log disk usage:	0%

Use Tablet as a Secondary Monitor

- Open the browser and go to https://training.fortinet.com
- Log in and find your Fast Track course that is in progress
- Access devices as normal



Upcoming Courses
Course: [Dynamic Clo
Lab Activity: FortiMai
training.fortinet.com/course/view.php?id=9893
FORTINET NSE Training Institute
Dashboard

[Dynamic Cloud Security] Advanced Email Security Solution with FortiMail v6.4 (Fast Track Session) - January 1, 2021

Introduction

FORTINET Fast Track Program

FORTINET®