Question #1 *Topic 1*

In the Secure Private Access (SPA) use case, which two FortiSASE features facilitate access to corporate applications? (Choose two.)

A. cloud access security broker (CASB)

B. SD-WAN

C. zero trust network access (ZTNA)

D. thin edge

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Which two components are part of onboarding a secure web gateway (SWG) endpoint for secure internet access (SIA)? (Choose two.)

A. proxy auto-configuration (PAC) file

B. FortiSASE certificate authority (CA) certificate

C. FortiClient software

D. tunnel policy

Suggested Answer: *AB*

Community vote distribution

AB (67%) AC (22%) 11%

SPAO 1 week ago

Selected Answer: D

Hi all,

Is this related with the exam NSE5 - FortiSASE and SD-WAN 7.6 Core Administrator? If not, can you please redirect me to the correct page ? Thanks

upvoted 1 times

1aeafe2 1 month, 2 weeks ago

Selected Answer: AB

A (Pag.46) Remote users configure FortiSASE as an explicit web proxy through their web browser or by using a proxy autoconfiguration (PAC) file.

B(Pag 47) You should provide users with the required certificate authority (CA) certificate and PAC file to connect to the FortiSASE gateway.

upvoted 2 times

darkstar15 2 months, 3 weeks ago

Selected Answer: AC

El CA SSL ya viene embebido dentro del PAC file.

upvoted 1 times

Gelicienta 2 months, 3 weeks ago

Selected Answer: AB

El archivo PAC se utiliza para redirigir el tráfico web del endpoint al proxy de FortiSASE, permitiendo aplicar políticas de seguridad.

El certificado CA de FortiSASE se instala en el endpoint para permitir la inspección de tráfico cifrado (SSL/TLS) sin generar alertas de seguridad en el navegador. El FortiClient es para Modo Agent, no SWG

upvoted 2 times

Reprintme 3 months ago

Selected Answer: AB

AB...FortiClient (C) is used for private access.

upvoted 2 times

tovich 3 months, 1 week ago

Selected Answer: AC

FortiSASE uses security web gateway for agentless scenario. And in this case, the user need to hace PAC file configure on its browser with FortiSASE CA for trusting SSL request before allowing traffic.

upvoted 1 times

Passam 1 week, 4 days ago

yes, therefore not C but B. coz it's agentless, no need forticlient.

upvoted 1 times

Question #3 *Topic 1*

Which two advantages does FortiSASE bring to businesses with microbranch offices that have FortiAP deployed for unmanaged devices? (Choose two.)

A. It secures internet access both on and off the network.

B. It uses zero trust network access (ZTNA) tags to perform device compliance checks.

C. It eliminates the requirement for an on-premises firewall.

D. It simplifies management and provisioning.

Suggested Answer: *AD*

Community vote distribution

AC (80%) AD (20%)

Mary56 1 month, 2 weeks ago

Selected Answer: AD

For microbranch offices with FortiAP deployed for unmanaged devices, FortiSASE provides:

Secure Internet Access Everywhere

FortiSASE applies consistent security policies whether the user is connected through the microbranch FortiAP or working remotely.
This eliminates gaps in protection for unmanaged devices.

Simplified Management and Provisioning

Centralized cloud-based management reduces complexity for small branches that lack dedicated IT staff.
No need for full firewall deployment or complex configurations at each microbranch.

upvoted 1 times

tovich 3 months, 1 week ago

Selected Answer: AC

In this case, tne key words is unmanaged devices. Thus the correct responses are A and C as the Firewall is not neccessary. Note also that the FortiAP has a different license subscription for FortiSASE SIA.

upvoted 4 times

Question #4 *Topic 1*

Which information can an administrator monitor using reports generated on FortiSASE?

A. sanctioned and unsanctioned Software-as-a-Service (SaaS) applications usage

B. FortiClient vulnerability assessment

C. SD-WAN performance

D. FortiSASE administrator and system events

Suggested Answer: *A*

Community vote distribution

B (100%)

Passam 1 week, 4 days ago

Selected Answer: B

In FortiSASE portal

Operations --> Reports --> Scheduled reports

Name:Endpoint Vulnerability Report

Description: Vulnerabilities detected through FortiClient scans throughout the network

So B

upvoted 1 times

Question #5 *Topic 1*

In a FortiSASE secure web gateway (SWG) deployment, which two features protect against web-based threats? (Choose two.)

A. SSL deep inspection for encrypted web traffic

B. malware protection with sandboxing capabilities

C. web application firewall (WAF) for web applications

D. intrusion prevention system (IPS) for web traffic

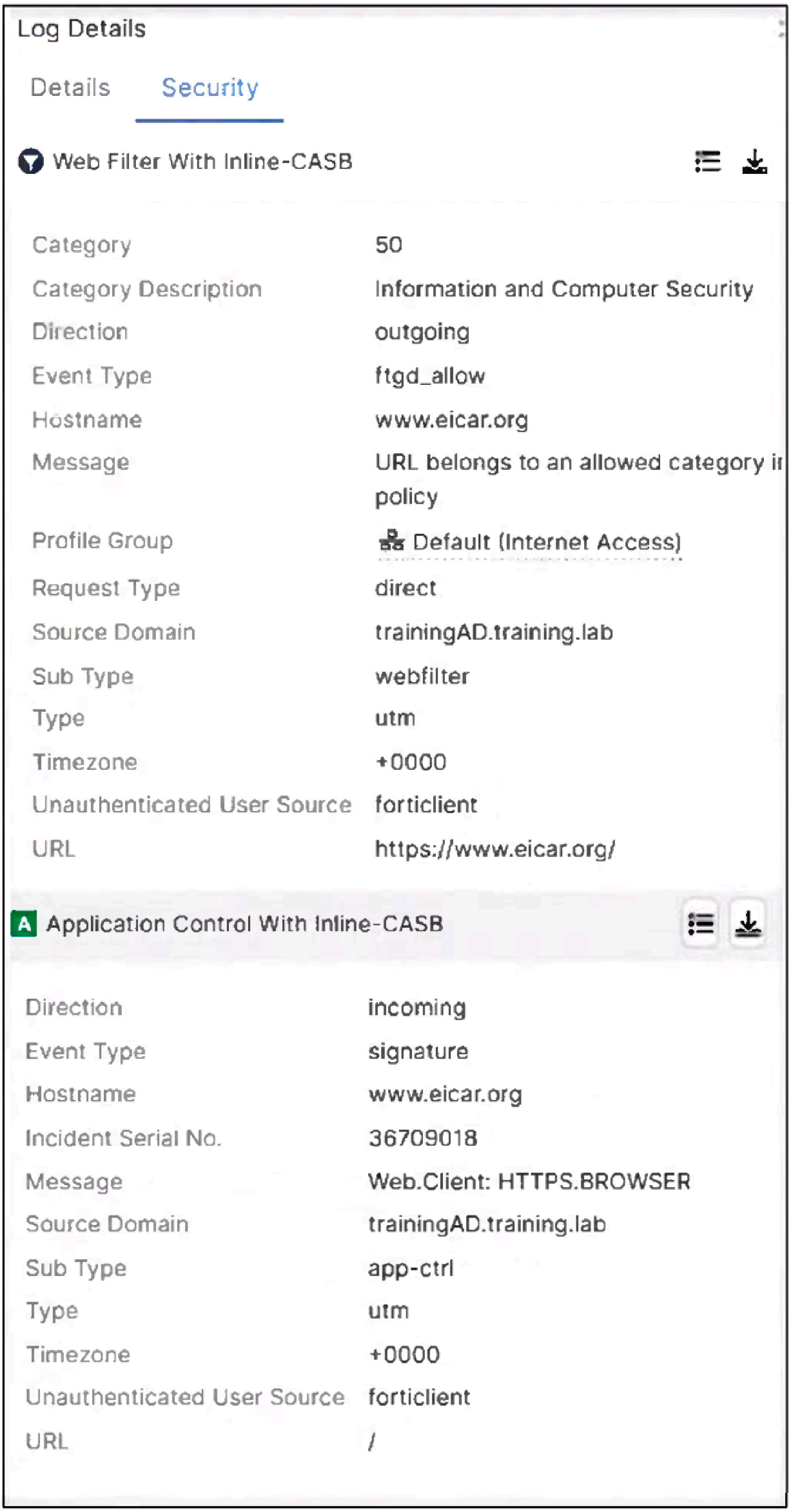
Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Refer to the exhibits.

Traffic logs



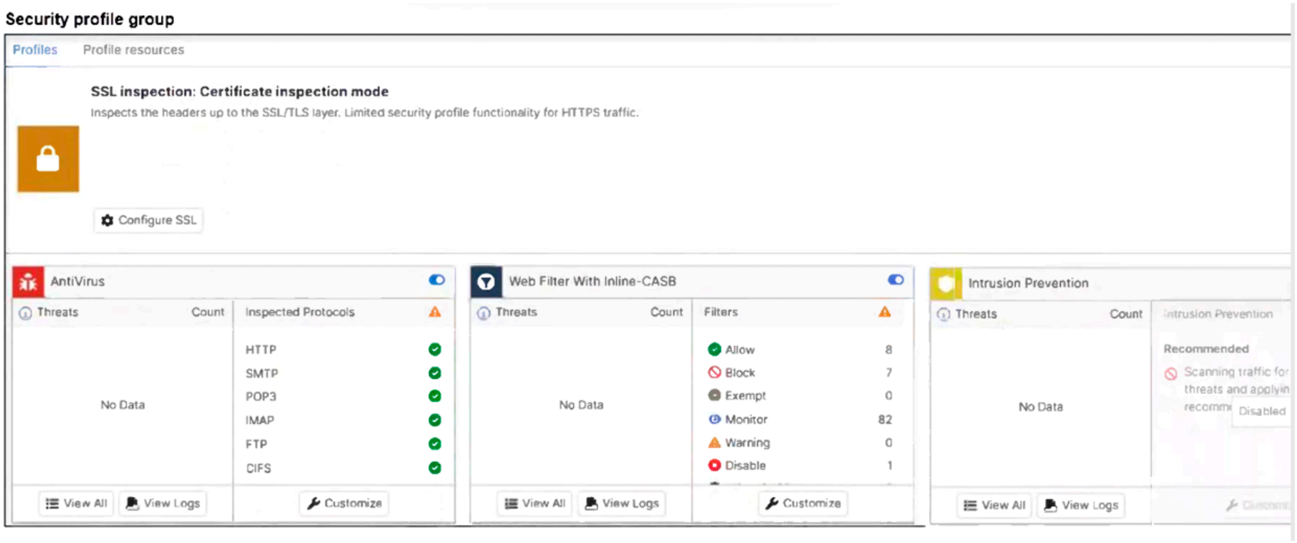
Log Details

Web Filter With Inline-CASB

Category	50
Category Description	Information and Computer Security
Direction	outgoing
Event Type	ftgd_allow
Hostname	www.eicar.org
Message	URL belongs to an allowed category ir policy
Profile Group	Default (Internet Access)
Request Type	direct
Source Domain	trainingAD.training.lab
Sub Type	webfilter
Type	utm
Timezone	+0000
Unauthenticated User Source	forticlient
URL	https://www.eicar.org/

A Application Control With Inline-CASB

Direction	incoming
Event Type	signature
Hostname	www.eicar.org
Incident Serial No.	36709018
Message	Web.Client: HTTPS.BROWSER
Source Domain	trainingAD.training.lab
Sub Type	app-ctrl
Type	utm
Timezone	+0000
Unauthenticated User Source	forticlient
URL	/



Security profile group

SSL inspection: Certificate inspection mode

Inspects the headers up to the SSL/TLS layer. Limited security profile functionality for HTTPS traffic.

AntiVirus

Threats	Count
No Data	

Inspected Protocols	⚠
HTTP	✓
SMTP	✓
POP3	✓
IMAP	✓
FTP	✓
CIFS	✓

Web Filter With Inline-CASB

Threats	Count
No Data	

Filters	⚠
Allow	8
Block	7
Exempt	0
Monitor	82
Warning	0
Disable	1

Intrusion Prevention

Threats	Count
No Data	

Intrusion Prevention

Recommended

Scanning traffic for threats and applyin recomm Disabled

A FortiSASE administrator has configured an antivirus profile in the security profile group and applied it to the internet access policy. Remote users are still able to download the eicar.com-zip file from https://eicar.org.

Which configuration on FortiSASE is allowing users to perform the download?

A. Web filter is allowing the URL.

B. Deep inspection is not enabled.

C. Application control is exempting all the browser traffic.

D. Intrusion prevention is disabled.

Suggested Answer: *B*

Community vote distribution

D (100%)

Passam 1 week, 4 days ago

Selected Answer: D

Intrusion prevention is inspected by Antivirus.

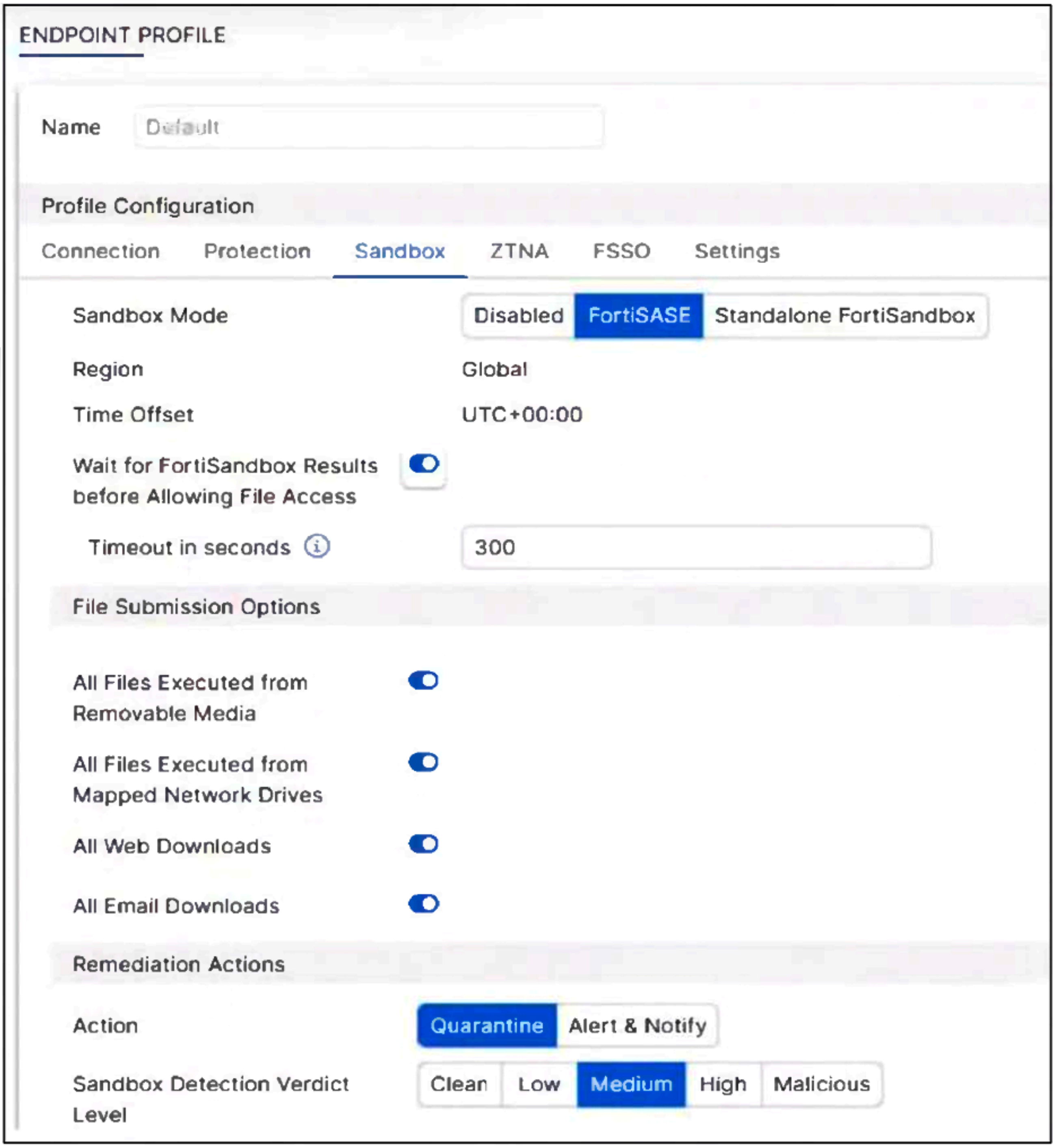
Antivirus is about scanning files

upvoted 1 times

Question #7

Topic 1

Refer to the exhibit.



ENDPOINT PROFILE

Name: Default

Profile Configuration

Sandbox Mode: Disabled [✓ FortiSASE] Standalone FortiSandbox

Region: Global

Time Offset: UTC+00:00

Wait for FortiSandbox Results before Allowing File Access: ●

Timeout in seconds: 300

File Submission Options

All Files Executed from Removable Media: ●

All Files Executed from Mapped Network Drives: ●

All Web Downloads: ●

All Email Downloads: ●

Remediation Actions

Action: [✓ Quarantine] Alert & Notify

Sandbox Detection Verdict Level: Clean Low [✓ Medium] High Malicious

Based on the configuration shown, in which two ways will FortiSASE process sessions that require FortiSandbox inspection? (Choose two.)

A. Only endpoints assigned a profile for sandbox detection will be processed by the sandbox feature.

B. FortiClient quarantines only infected files that FortiSandbox detects as medium level.

C. All files executed on a USB drive will be sent to FortiSandbox for analysis.

D. All files will be sent to a on-premises FortiSandbox for inspection.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

An administrator must restrict endpoints from certain countries from connecting to FortiSASE.
Which configuration can achieve this?

A. Configure a network lockdown policy on the endpoint profiles.

B. Configure a geography address object as the source for a deny policy.

C. Configure geofencing to restrict access from the required countries.

D. Configure source IP anchoring to restrict access from the specified countries.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

What is the benefit of SD-WAN on-ramp deployment with FortiSASE?

A. To provide access to private applications using the bookmark portal

B. To provide device compliance checks using ZTNA tags

C. To secure internet traffic for branch users

D. To manage branch location endpoints

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which two settings are automatically pushed from FortiSASE to FortiClient in a new FortiSASE deployment with default settings? (Choose two.)

A. zero trust network access (ZTNA) tags

B. tunnel profile

C. FortiSASE certificate authority (CA) certificate

D. real-time protection

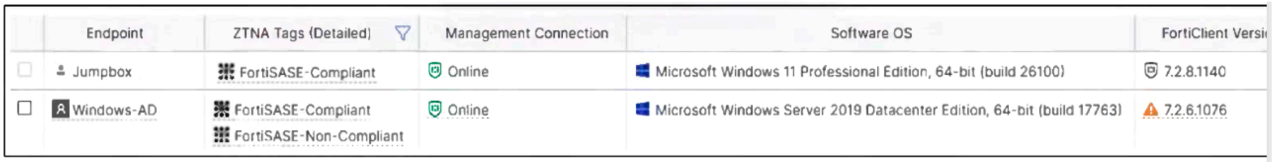
Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

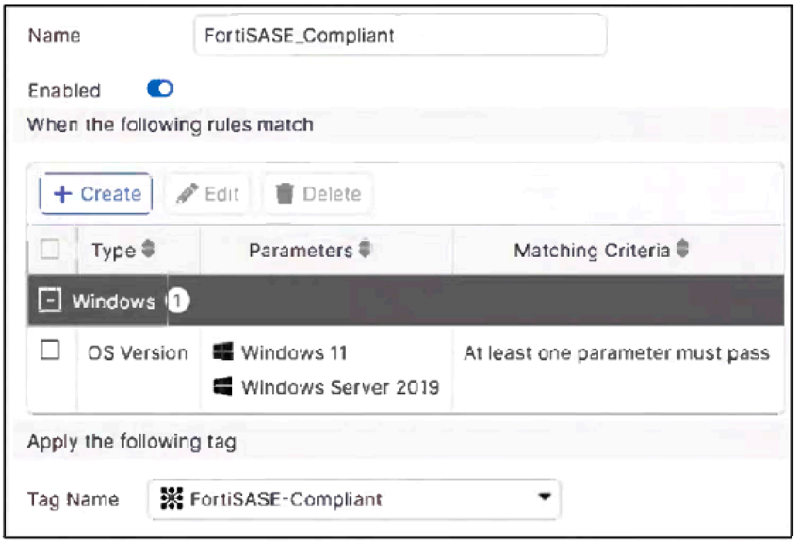
Refer to the exhibits.

Managed Endpoints



	Endpoint	ZTNA Tags (Detailed)	Management Connection	Software OS	FortiClient Versi
□	Jumpbox	FortiSASE-Compliant	Online	Microsoft Windows 11 Professional Edition, 64-bit (build 26100)	7.2.8.1140
□	Windows-AD	FortiSASE-Compliant FortiSASE-Non-Compliant	Online	Microsoft Windows Server 2019 Datacenter Edition, 64-bit (build 17763)	⚠ 7.2.6.1076

ZTNA Tagging Rules



Name: FortiSASE_Compliant

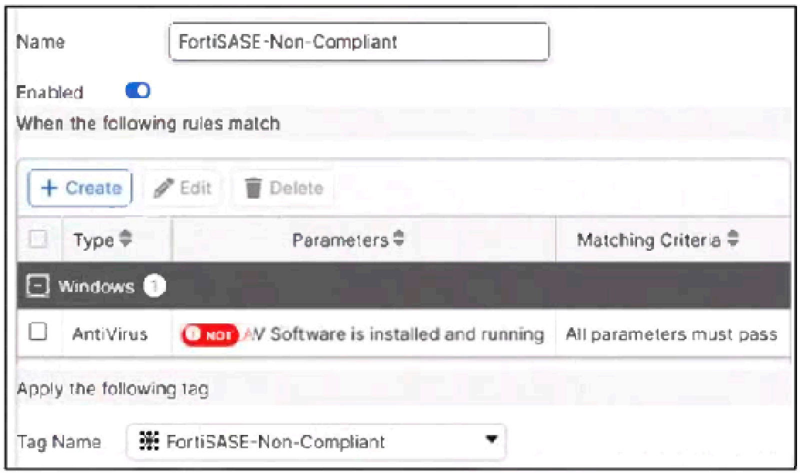
Enabled: ●

When the following rules match

□	Type	Parameters	Matching Criteria
□	Windows 1		
□	OS Version	Windows 11 Windows Server 2019	At least one parameter must pass

Apply the following tag

Tag Name: FortiSASE-Compliant



Name: FortiSASE-Non-Compliant

Enabled: ●

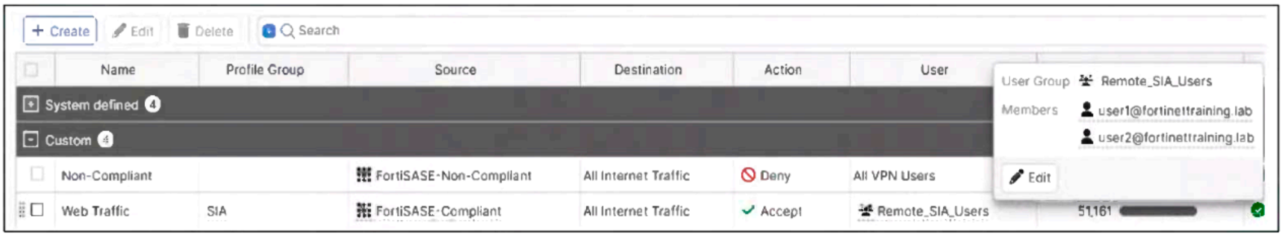
When the following rules match

□	Type	Parameters	Matching Criteria
□	Windows 1		
□	AntiVirus	NOT AV Software is installed and running	All parameters must pass

Apply the following tag

Tag Name: FortiSASE-Non-Compliant

Secure Internet Access Policy



□	Name	Profile Group	Source	Destination	Action	User	
	System defined 4						
	Custom 4						
□	Non-Compliant		FortiSASE-Non-Compliant	All Internet Traffic	Deny	All VPN Users	
□	Web Traffic	SIA	FortiSASE-Compliant	All Internet Traffic	✓ Accept	Remote_SIA_Users	51,161

User Group: Remote_SIA_Users

Members: user1@fortinettraining.lab
user2@fortinettraining.lab

Jumpbox and Windows-AD are endpoints from the same remote location. Jumpbox can access the internet through FortiSASE, while Windows-AD can no longer access the internet.

Based on the information in the exhibits, which reason explains the outage on Windows-AD?

A. Windows-AD is excluded from FortiSASE management.

B. The FortiClient version installed on Windows AD does not match the expected version on FortiSASE.

C. The device posture for Windows-AD has changed.

D. The remote VPN user on Windows-AD no longer matches any VPN policy.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which description of the FortiSASE inline-CASB component is true?

A. It has limited visibility when data is transmitted.

B. It detects data in motion.

C. It is placed outside the traffic path.

D. It relies on API to integrate with cloud services.

Suggested Answer: *B*

Community vote distribution

B (100%)

U2D2A2R2A 3 weeks, 5 days ago

Selected Answer: B

B is correct

upvoted 1 times

Question #13 *Topic 1*

Which authentication method overrides any other previously configured user authentication on FortiSASE?

A. MFA

B. Local

C. RADIUS

D. SSO

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

What are two advantages of using zero-trust tags? (Choose two.)

A. Zero-trust tags can determine the security posture of an endpoint.

B. Zero-trust tags can be assigned to endpoint profiles based on user groups.

C. Zero-trust tags can be used to allow or deny access to network resources.

D. Zero-trust tags can help monitor endpoint system resource usage.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Which FortiSASE feature ensures least-privileged user access to corporate applications that are protected by an on-premises FortiGate device?

A. secure web gateway (SWG)

B. zero trust network access (ZTNA)

C. cloud access security broker (CASB)

D. remote browser isolation (RBI)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 Topic 1

A company must provide access to a web server through FortiSASE secure private access for contractors.
What is the recommended method to provide access?

A. Configure a TCP access proxy forwarding rule and push it to the contractor FortiClient endpoint.

B. Update the DNS records on the endpoint to access private applications.

C. Publish the web server URL on a bookmark portal and share it with contractors.

D. Update the PAC file with the web server URL and share it with contractors.

Suggested Answer: *C*

Community vote distribution

C (100%)

Mary56 1 month, 2 weeks ago

Selected Answer: C

TCP Access Proxy Forwarding Rule: This creates a secure tunnel between the contractor's FortiClient and the FortiSASE service, which then forwards traffic to the internal web server. This ensures:

Strong authentication and policy enforcement.
No need to modify DNS or PAC files manually.
No exposure of internal URLs on public portals.
upvoted 1 times

Question #17 *Topic 1*

Your FortiSASE customer has a small branch office in which ten users will be using their personal laptops and mobile devices to access the internet.
Which deployment should they use to secure their internet access with minimal configuration?

A. Deploy FortiGate as a LAN extension to secure internet access.

B. Deploy FortiAP to secure internet access.

C. Deploy FortiClient endpoint agent to secure internet access.

D. Deploy SD-WAN on-ramp to secure internet access.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Which information does FortiSASE use to bring network lockdown into effect on an endpoint?

A. Zero-day malware detection on endpoint

B. The number of critical vulnerabilities detected on the endpoint

C. The security posture of the endpoint based on ZTNA tags

D. The connection status of the tunnel to FortiSASE

Suggested Answer: *D*

Community vote distribution

D (83%) C (17%)

Emre84 1 week, 3 days ago

Selected Answer: C

Network lockdown is an intentional restriction enforced while the tunnel is still up:

Endpoint is connected

Tunnel is established

FortiSASE is reachable

Access is restricted because the endpoint is no longer trusted

That trust decision comes from ZTNA tags.

upvoted 1 times

Bluegrass168 1 week, 5 days ago

Selected Answer: D

https://docs.fortinet.com/document/forticlient/7.2.0/new-features/127394/network-lockdown-for-off-fabric-endpoints-7-2-1

"You can configure network lockdown for off-fabric endpoints when they are not connected to SSL VPN."

upvoted 1 times

Racoon1 1 month, 1 week ago

Selected Answer: D

Based on the FortiSASE 25 Administrator Study Guide (page 135), network lockdown is triggered based on the connection status of the FortiSASE tunnel combined with on-net/off-net detection, not directly by ZTNA tags, vulnerabilities, or malware detection.

upvoted 1 times

Dranizz 2 months ago

Selected Answer: D

Network lockdown occurs when Forticlient is either off-net or VPN to FortiSASE is disconnected

upvoted 3 times

Question #19 *Topic 1*

For monitoring potentially unwanted applications on endpoints, which information is available on the FortiSASE software installations page?

A. the vendor of the software

B. the endpoint the software is installed on

C. the license status of the software

D. the usage frequency of the software

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

What is the recommended method to upgrade FortiClient in a FortiSASE deployment?

A. Remote users must upgrade the FortiClient manually.

B. FortiSASE automatically upgrades FortiClient when a new version is released.

C. The FortiSASE administrator must assign endpoint groups to an endpoint upgrade rule.

D. The FortiSASE administrator will upload the desired FortiClient version to the FortiSASE portal and push it to endpoints.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Which two are required to enable central management on FortiSASE? (Choose two.)

A. FortiSASE connector configured on FortiManager.

B. FortiManager and FortiSASE registered under the same FortiCloud account.

C. The FortiManager IP address in the FortiSASE central management configuration.

D. FortiSASE central management entitlement applied to FortiManager.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which FortiSASE component protects users from online threats by hosting their browsing sessions on a remote container within a secure environment?

A. secure web gateway (SWG)

B. remote browser isolation (RBI)

C. cloud access security broker (CASB)

D. data loss prevention (DLP)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

What are two benefits of deploying FortiSASE with FortiGate ZTNA access proxy? (Choose two.)

A. It offers data center redundancy.

B. The on-premises FortiGate performs a device posture check.

C. It is ideal for latency-sensitive applications.

D. It supports both agentless ZTNA and agent-based ZTNA.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

In a FortiSASE SD-WAN deployment with dual hubs, what are two benefits of assigning hubs with different priorities? (Choose two.)

A. optimized performance that meets the minimum SLA requirements

B. load balancing based on session identification

C. bandwidth allocated traffic shaping

D. redundancy to seamlessly steer traffic

Suggested Answer: *AD*

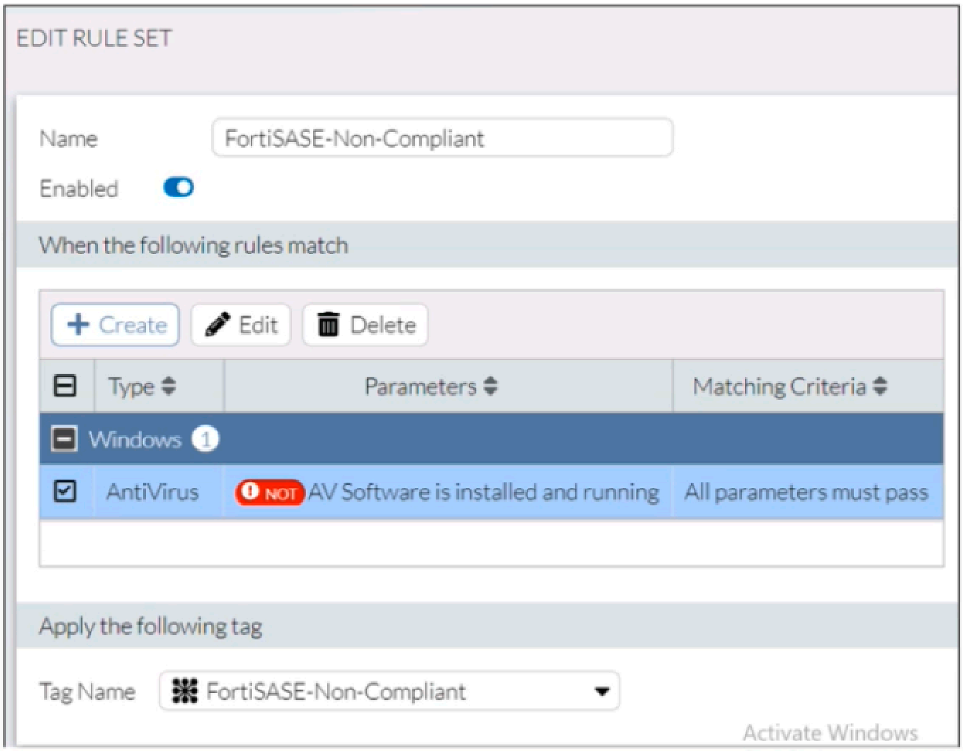
Currently there are no comments in this discussion, be the first to comment!

Question #25

Topic 1

Refer to the exhibits.

FortiSASE Non-Compliant



EDIT RULE SET

Name: FortiSASE-Non-Compliant

Enabled: ●

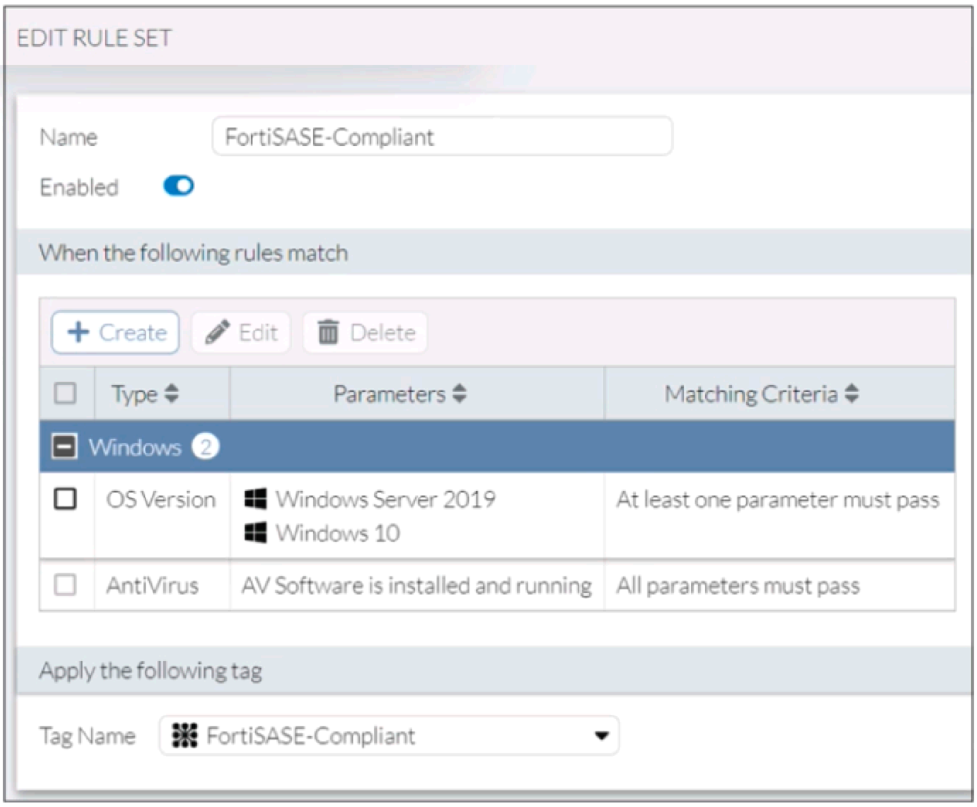
When the following rules match

⊟	Type	Parameters	Matching Criteria
⊟	Windows 1		
☑	AntiVirus	NOT AV Software is installed and running	All parameters must pass

Apply the following tag

Tag Name FortiSASE-Non-Compliant

FortiSASE Compliant



EDIT RULE SET

Name: FortiSASE-Compliant

Enabled: ●

When the following rules match

□	Type	Parameters	Matching Criteria
⊟	Windows 2		
□	OS Version	Windows Server 2019 Windows 10	At least one parameter must pass
□	AntiVirus	AV Software is installed and running	All parameters must pass

Apply the following tag

Tag Name FortiSASE-Compliant

Antivirus is installed on a Windows 10 endpoint, but the windows application firewall is stopping it from running.

What will the endpoint security posture check be?

A. FortiClient will tag the endpoint as FortiSASE-Non-Compliant.

B. FortiClient will be unmanaged from FortiSASE due to failed compliance.

C. FortiClient will trigger network lockdown on the endpoint.

D. FortiClient will prompt the user to enable antivirus.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!