Question #1 *Topic 1*

Which two are valid traffic processing actions that a FortiSwitch access control list (ACL) can apply to matching traffic? (Choose two.)

A. Redirect frames to another port.

B. Assign traffic to a high-priority egress queue.

C. Encrypt frames.

D. Drop frames.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

SCC4exams 1 month, 1 week ago

Selected Answer: AD

Correct answer A&D

upvoted 1 times

Clauster 3 months ago

Selected Answer: AD

Answers are A and D.

upvoted 1 times

79fad4e 3 months, 2 weeks ago

Selected Answer: AD

Based on Fortiswitch 7.6 page 358 traffic processing : count , drop , redirect , or mirror frames

upvoted 2 times

bas07 4 months, 3 weeks ago

Selected Answer: BD

Yes, Correct Answer: BD

upvoted 1 times

Question #2 *Topic 1*

Which two statements about 802.1X authentication on FortiSwitch ports are true? (Choose two.)

A. In port-based 802.1x, all hosts behind an authenticated port are allowed access after a successful authentication.

B. A port policy is used to apply 802.1x authentication on a FortiSwitch interface.

C. 802.1X authentication can be applied only to trunk ports and not access ports.

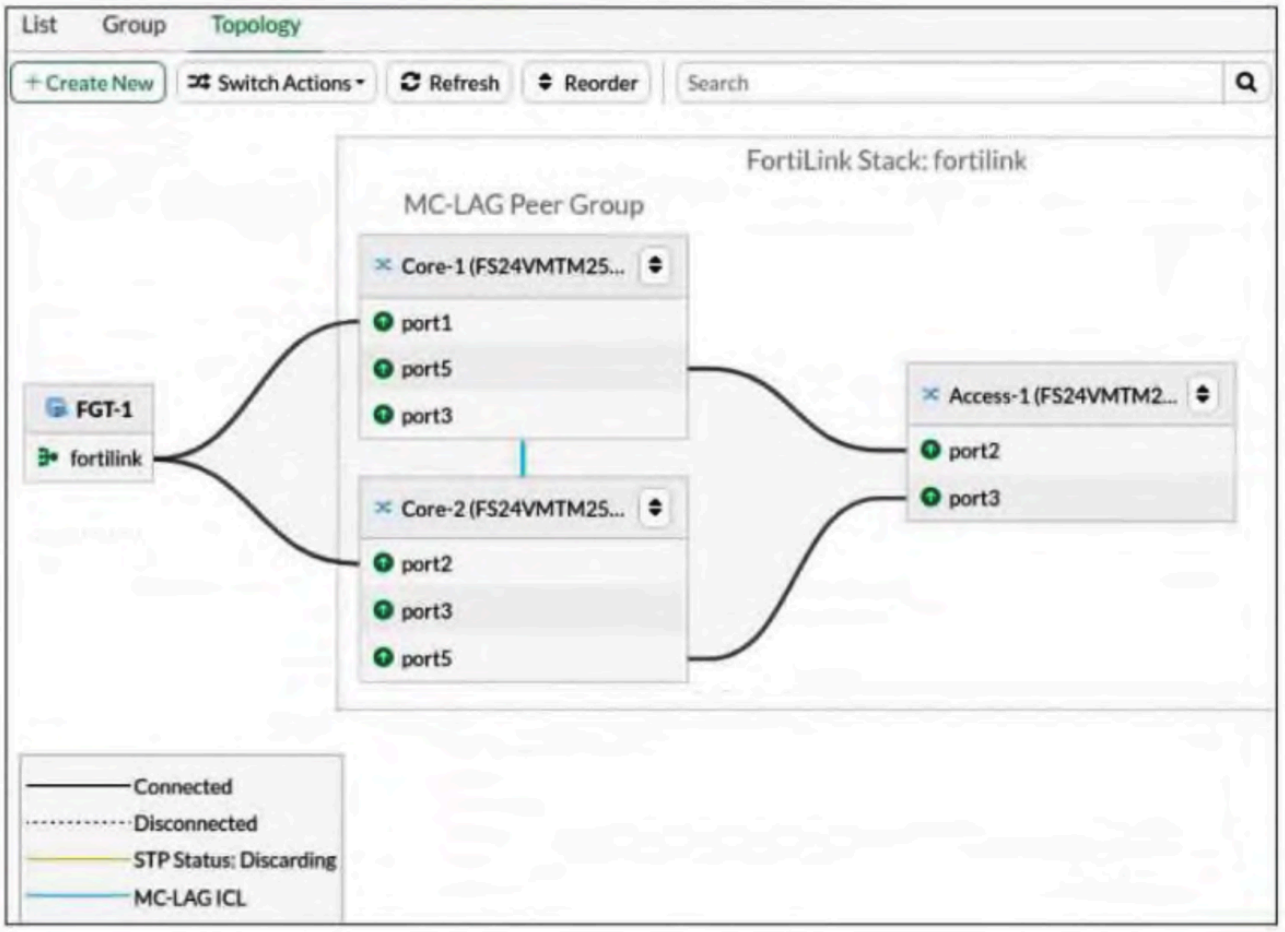
D. All devices connecting to FortiSwitch must support 802.1X authentication.

Suggested Answer: *AB*

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

Refer to the exhibits.

Topology view -



Core-1 CLI output -

```
FGT-1 # diagnose switch-controller switch-info stp Core-1
Vdom: root

Core-1:

MST Instance Information, primary-Channel:

Instance ID 0 (CST)
  Config          Priority 20480
                  Bridge MAC 02090f000701, MD5 Digest 9999b43d77cc58bba8854f9991c4a487

  Root            MAC 02090f000701, Priority 20480, Path Cost 0, Remaining Hops 20
                  (This bridge is the root)

  Regional Root   MAC 02090f000701, Priority 20480, Path Cost 0
                  (This bridge is the regional root)
```

Core-2 CLI output -

```
Core-2:

MST Instance Information, primary-Channel:

Instance ID 0 (CST)
  Config         Priority 20480
                 Bridge MAC 02090f000701, MD5 Digest 9999b43d77cc58bba8854f9991c4a487

  Root           MAC 02090f000701, Priority 20480, Path Cost 0, Remaining Hops 20
                 (This bridge is the root)

  Regional Root  MAC 02090f000701, Priority 20480, Path Cost 0
                 (This bridge is the regional root)

  Active Times   Forward Time 15, Max Age 20, Remaining Hops 20
```

An administrator has deployed two FortiSwitch devices, Core-1 and Core-2, as multichassis link aggregation group (MCLAG) peers. These switches are connected to FortiGate for FortiLink and to an access switch (Access-1) using an inter-switch link (ISL). After configuration, the administrator notices that both Core-1 and Core-2 are claiming to be the root bridge in the Multiple Spanning Tree Protocol (MSTP) topology. What explains this behavior?

A. FortiGate participates in MSTP and causes both switches to assume the root bridge role.

B. The ISL was not configured correctly, leading to MSTP inconsistency.

C. Both switches share the same bridge ID because MCLAG treats them as one logical switch.

D. MCLAG automatically disables STP on all peer switches.

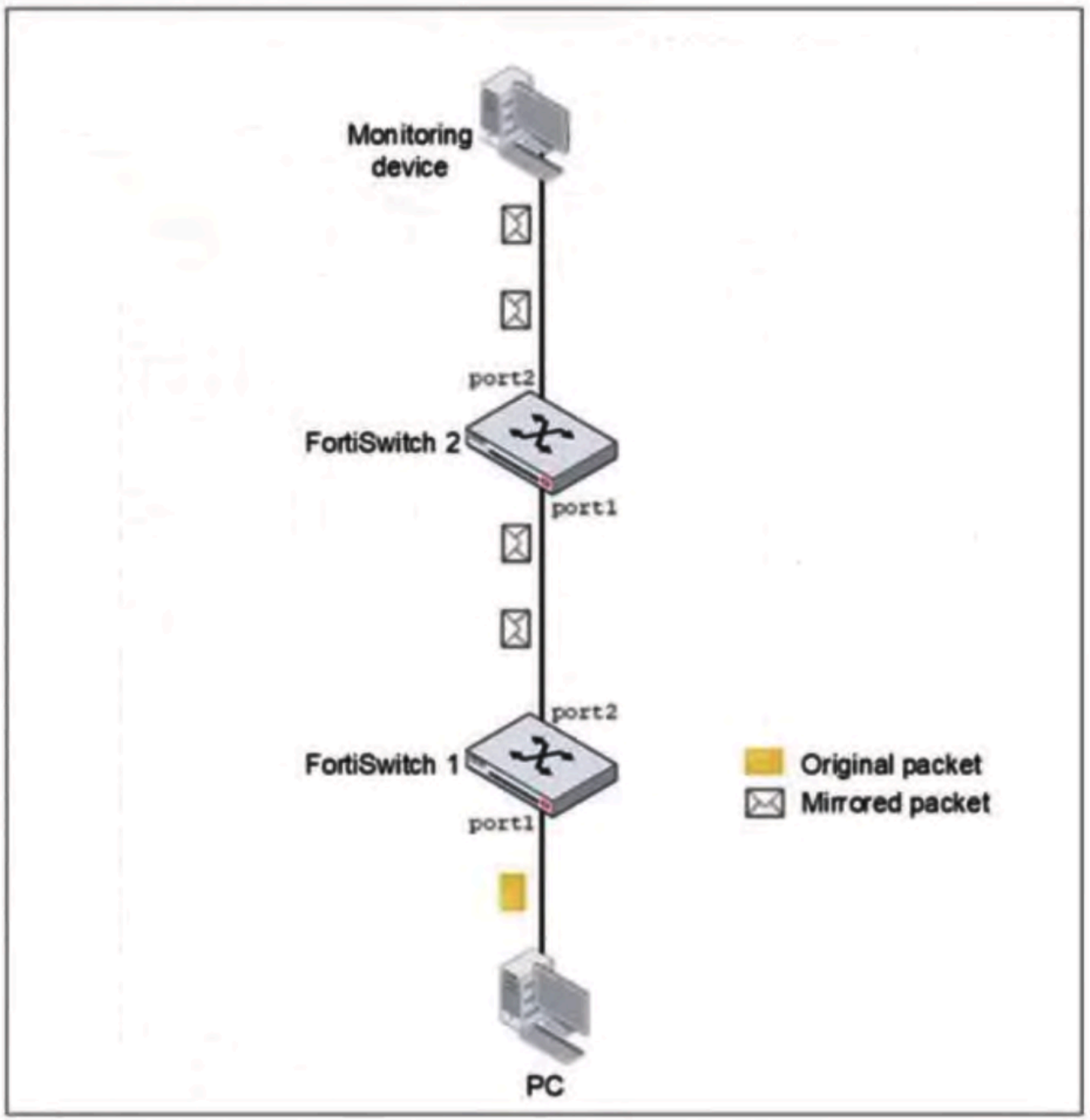
Suggested Answer: *C*

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

Question #4 *Topic 1*

Refer to the exhibit.

Network Topology -



You configured Switched Port Analyzer (SPAN) to monitor traffic from a source port on FortiSwitch 1, but the monitoring device is connected to FortiSwitch 2. After port mirroring configuration on FortiSwitch 1, the monitoring device is not receiving any mirrored traffic.
What is the most likely reason the mirrored traffic is not reaching the monitoring device?

A. SPAN does not support forwarding mirrored traffic across multiple switches.

B. SPAN traffic must be filtered with an access control list (ACL).

C. The SPAN session must be restarted after configuration.

D. The monitoring device must use a management IP in the same subnet.

Suggested Answer: *A*

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

Question #5 *Topic 1*

What happens if FortiSwitch fails to discover either FortiEdge Cloud or a FortiGate with FortiLink?

A. It switches to FortiLink mode by default.

B. It remains in local management mode.

C. It requires manual reimaging.

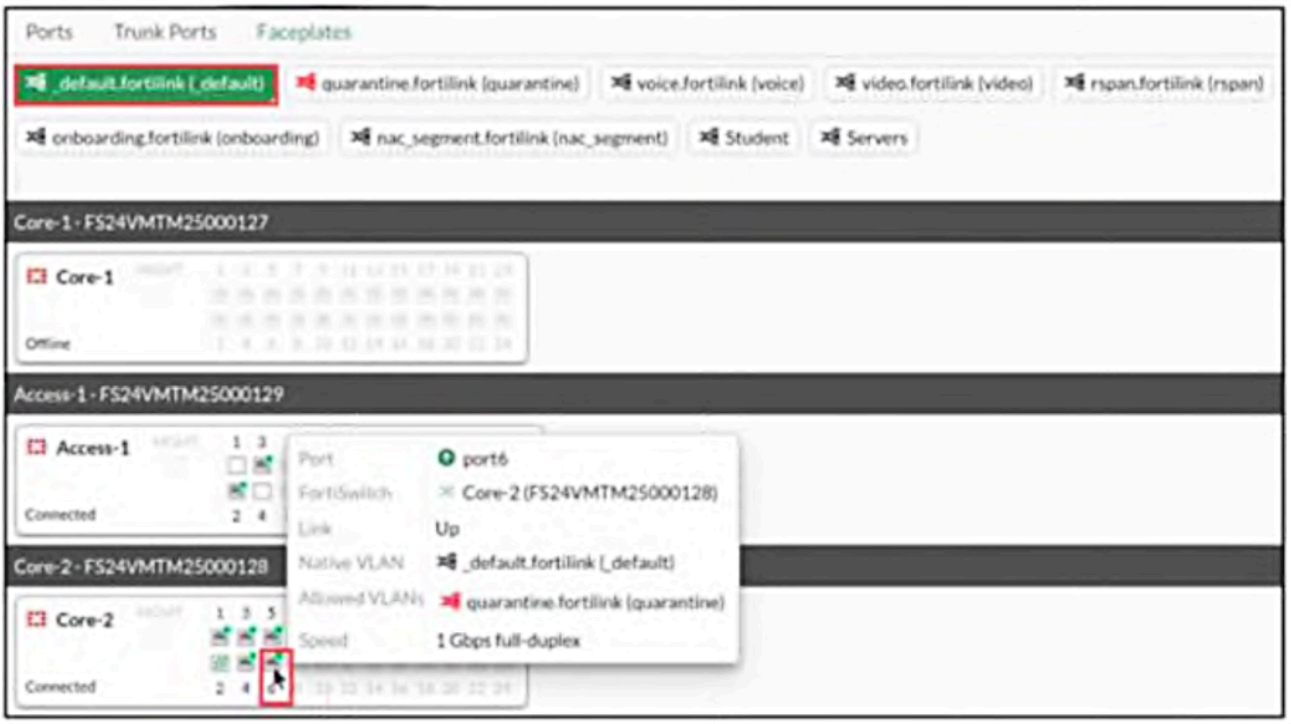
D. It disables auto-network.

Suggested Answer: *B*

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

Question #6 *Topic 1*

Refer to the exhibit.



Which information does FortiGate use to generate the port details in the FortiSwitch Faceplates view?

A. The FortiSwitch model

B. The Cisco Discovery Protocol (CDP) advertisements from FortiSwitch

C. The LLDP advertisements received from the FortiSwitch

D. The FortiLink discovery frames sent by FortiSwitch

Suggested Answer: *C*

Cesaru888 1 month, 3 weeks ago

Selected Answer: D

D is true. The guide states this in two places: the FortiLink discovery frames broadcast by FortiSwitch during switch discovery contain the list of ports on the switch and their type, and FortiOS uses this information to build the faceplate shown on the Faceplates tab of the FortiSwitch Ports page. The troubleshooting lesson reiterates it — FortiGate uses the switch port information included in the FortiLink discovery frames to build the faceplate image shown on the GUI.

upvoted 2 times

lukaszam 2 months ago

Selected Answer: D

Based on the official Fortinet training material, the correct answer is D. The FortiLink discovery frames broadcast by the switch contain the complete list of ports and their types, which FortiOS uses to structurally build the faceplate view in the GUI.

upvoted 2 times

Question #7 *Topic 1*

Refer to the exhibit.

Diagnose output -

```
Core-1 # diagnose switch physical-ports summary

  Portname    Status  Tpid  Vlan  Duplex  Speed  Flags          Discard
  _________   ______  ____  ____  ______  _____  _____________  _______

  port1       up      8100  4094  full    1G     QS,TL,         none
  port2       up      8100  1     full    1G     QS,  ,         none
  port3       up      8100  1     full    1G     QS,  ,         none
  port4       up      8100  1     full    1G     QS,  ,         none
  port5       up      8100  4094  full    1G     QS,TL,         none
  port6       down    8100  1     full    1G     QS,  ,         none
  port7       down    8100  1     full    1G     QS,  ,         none
  port8       down    8100  1     full    1G     QS,  ,         none
  port9       down    8100  1     full    1G     QS,  ,         none
  port10      down    8100  1     full    1G     QS,  ,         none
  port11      down    8100  1     full    1G     QS,  ,         none
  port12      down    8100  1     full    1G     QS,  ,         none
  port13      down    8100  1     full    1G     QS,  ,         none
  port14      down    8100  1     full    1G     QS,  ,         none
  port15      down    8100  1     full    1G     QS,  ,         none
  port16      down    8100  1     full    1G     QS,  ,         none
  port17      down    8100  1     full    1G     QS,  ,         none
  port18      down    8100  1     full    1G     QS,  ,         none
  port19      down    8100  1     full    1G     QS,  ,         none
  port20      down    8100  1     full    1G     QS,  ,         none
  port21      down    8100  1     full    1G     QS,  ,         none
  port22      down    8100  1     full    1G     QS,  ,         none
  port23      down    8100  1     full    1G     QS,  ,         none
  port24      down    8100  1     full    1G     QS,  ,         none
  internal    up      8100  4094  full    1G       ,  ,         none

  Flags: QS(802.1Q) QE(802.1Q-in-Q,external) QI(802.1Q-in-Q,internal)
  TS(static trunk) TF(forti trunk) TL(lacp trunk); MD(mirror dst)
  MI(mirror ingress) ME(mirror egress) MB(mirror ingress and egress)
  CF (Combo Fiber), CC (Combo Copper) LL(LoopBack Local) LR(LoopBack Remote)
```

The command diagnose switch physical-ports summary is executed on FortiSwitch.
Based on the VLAN assignments shown in the output, what is the most likely management configuration of this FortiSwitch?

A. FortiSwitch is managed by FortiSwitch Cloud.

B. FortiSwitch is managed by FortiGate.

C. FortiSwitch is operating in standalone mode.

D. FortiSwitch is operating in local mode.

Suggested Answer: *B*

freezingmaster 2 weeks, 2 days ago

Selected Answer: B

Port 4094 is used for FortiManagment - Auth,discovery,fortilink,and fortimanagment.

FortiCloud Switch - is managed of port 443

upvoted 1 times

Question #8 *Topic 1*

An administrator must deploy managed FortiSwitch devices in a remote location where multiple VLANs must be used to segment devices. No layer 3 switch or router is present at the site, and the only WAN connectivity is an ISP-provided router connected to the public internet.
Which two components are required to enable VLAN segmentation across this remote site? (Choose two.)

A. FortiGate and FortiSwitch configured with VXLAN to tunnel VLANs over the WAN

B. A layer 3 router at the remote location to handle inter-VLAN routing

C. A FortiSwitch model that supports VXLAN hardware acceleration

D. FortiSwitch and FortiGate devices configured with IPsec interfaces

E. FortiGate with a layer 3 interface to terminate the VXLAN overlay

Suggested Answer: *DE*

freezingmaster 2 weeks, 2 days ago

Selected Answer: AE

A. FortiGate and FortiSwitch configured with VXLAN to tunnel VLANs over the WAN
*This is the recommended method for managing fortiswitches with no Router at a remote cite.
B - no - this is a work around for the question
C. no - VXLAN hardware acceleration - What is that? no... it's not this.
D. no - IPsec interfaces vxlan is nat supported, also no router exists at remote local. - no
E. FortiGate with a layer 3 interface to terminate the VXLAN overlay. - on the main cite, this is needed for vxlan to work.

Therefore - A,E is my answer - corrections welcome.
upvoted 1 times

wooorkly 2 weeks, 5 days ago

Selected Answer: AD

A. FortiGate and FortiSwitch with VXLAN for VLAN tunneling over the WAN is correct.
Since there is no Layer 3 device on-site for inter-VLAN routing, the only way to maintain segmentation is to encapsulate Layer 2 VLAN traffic in VXLAN and forward it over the Layer 3 network (Internet) back to the central FortiGate, which will act as the Layer 3 gateway/inter-VLAN routing device. This is Fortinet's standard architecture for remote FortiSwitches without a local Layer 3 device.
D. FortiSwitch and FortiGate with configured IPsec interfaces is correct.
Since the only WAN connection is to the public Internet via an ISP router, FortiLink and VXLAN traffic must be protected as it traverses an untrusted network. Therefore, an IPsec tunnel is built between the FortiSwitch (or FortiExtender on-site) and the FortiGate, and a VXLAN overlay is placed on top of it to transmit VLANs.
upvoted 1 times

freezingmaster 2 weeks, 2 days ago

I agree this is secure, but it is not REQUIRED... How is the ipsec going to work if there is no router at the remote location? (Thanks for the discussion, but I dont reckon D is an answer).
upvoted 1 times

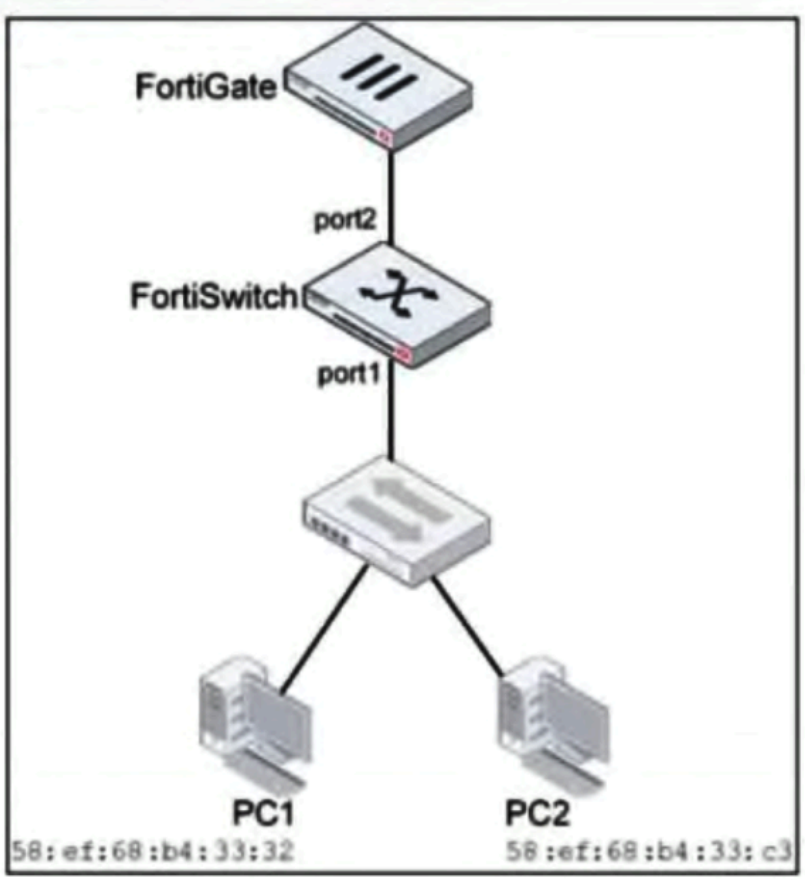
f2ed534 1 month ago

Selected Answer: AE

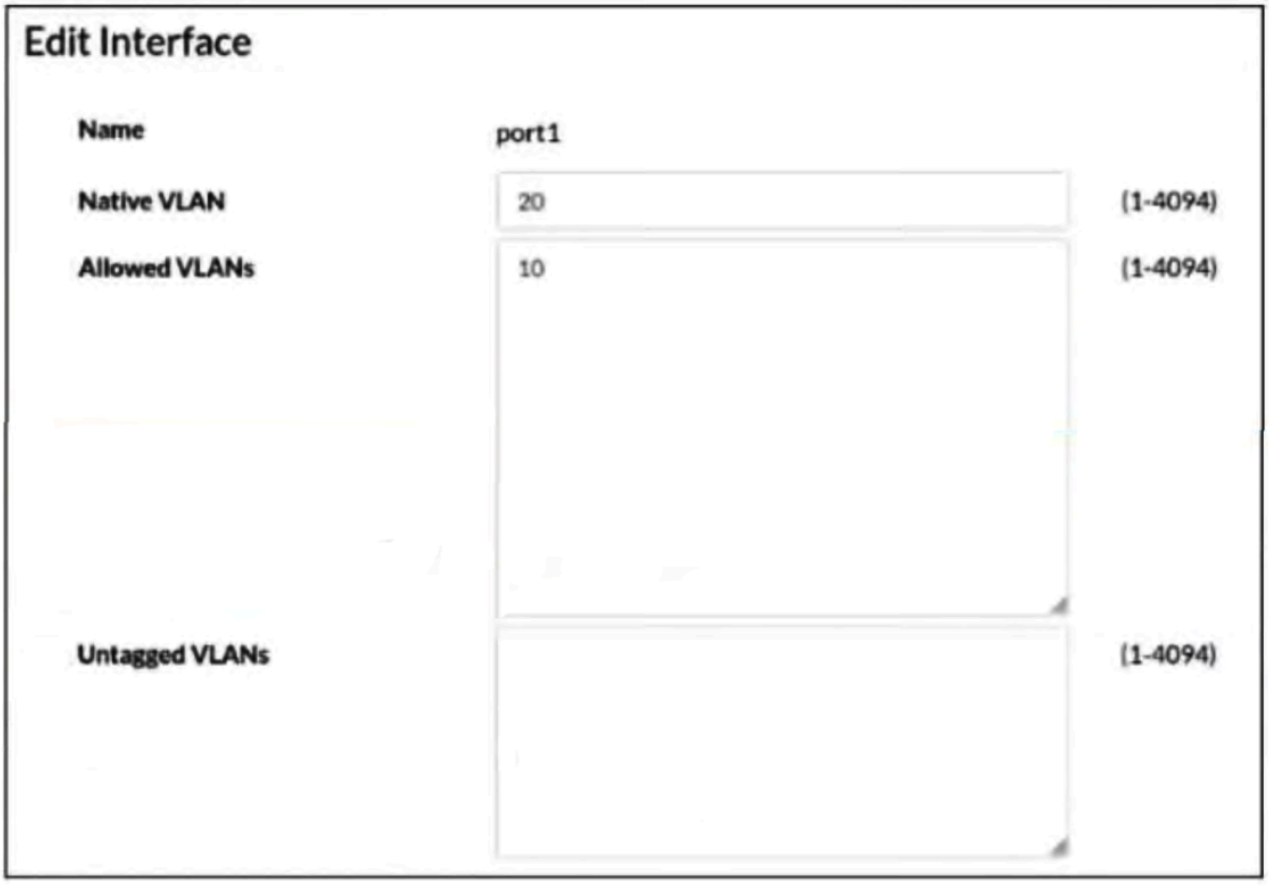
Based on the NSE 5 FortiSwitch 7.6 Study Guide, the correct answers are:
A. FortiGate and FortiSwitch configured with VXLAN to tunnel VLANs over the WAN
E. FortiGate with a layer 3 interface to terminate the VXLAN overlay.
upvoted 2 times

Refer to the exhibits.

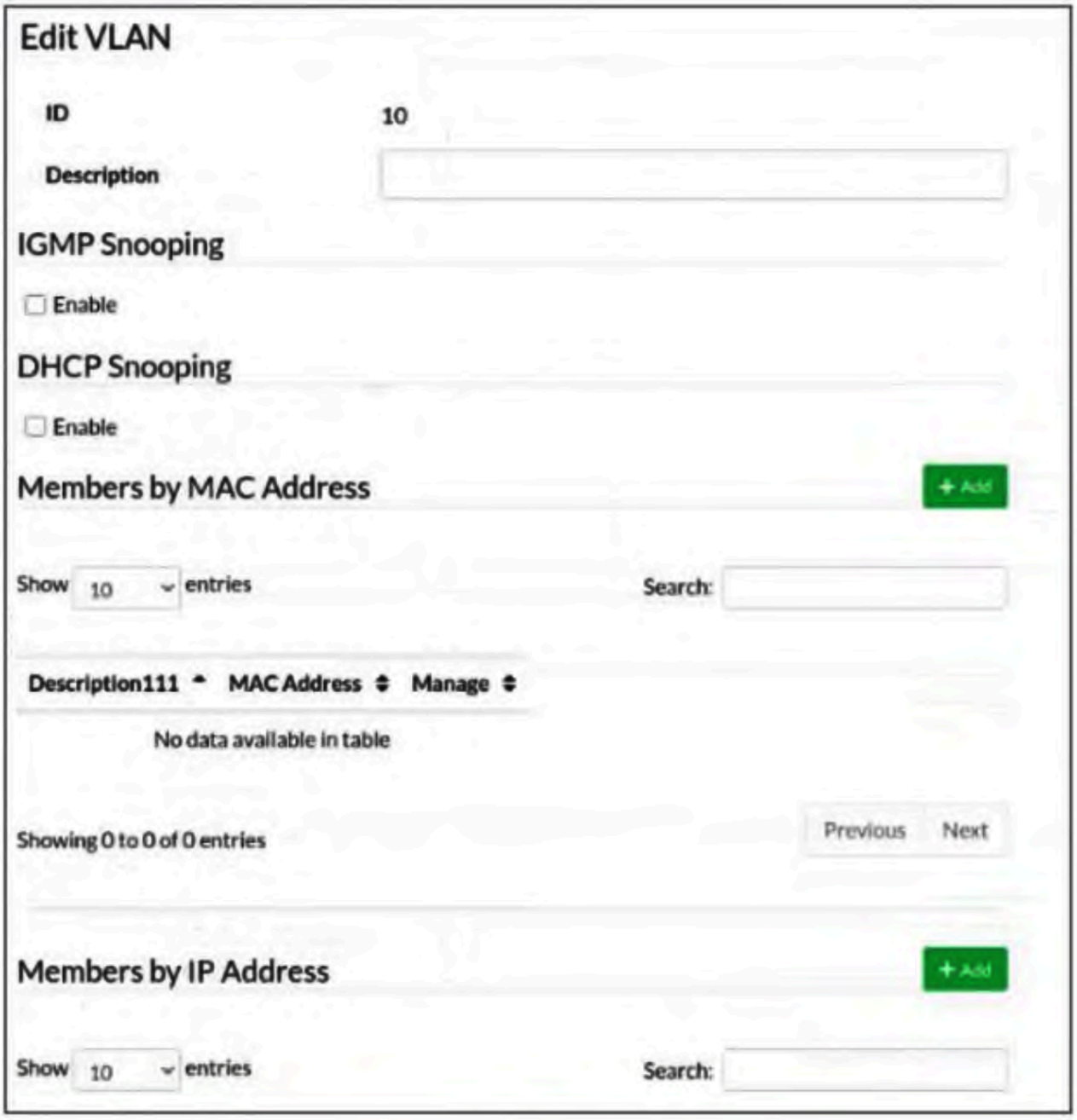
Network topology -



Interface configuration -



VLAN configuration -



Traffic arriving on port2 on FortiSwitch is tagged with VLAN ID 10 and destined for PC1 connected on port1. PC1 expects to receive traffic untagged from port1 on FortiSwitch.
Which two configurations can you perform on FortiSwitch to ensure PC1 receives untagged traffic on port1? (Choose two.)

A. Add VLAN ID 10 as a member of the untagged VLANs on port1.

B. Include VLAN 10 and VLAN 20 as allowed VLANs on port1.

C. Add the MAC address of PC1 as a member of VLAN 10.

D. Remove VLAN 10 from the allowed VLANs and add it to untagged VLANs on port1.

Suggested Answer: *AC*

SCC4exams 1 month ago

Selected Answer: AC

Correct answer A&C

I agree with cb9a70b

upvoted 1 times

cb9a70b 2 months, 1 week ago

Selected Answer: AC

A: By adding VLAN ID 10 to the Untagged VLANs field on port1, you are modifying the egress behavior of that specific port. When traffic for VLAN 10 is destined to leave out of port1, the FortiSwitch strips off the 802.1Q VLAN tag before forwarding the frame to the wire. As a result, PC1 receives the packet completely untagged.

C: As shown in the configuration screenshots, port1 has Native VLAN 20 and Allowed VLAN 10.
In FortiSwitch's MAC-based VLAN architecture, if you add PC1's specific MAC address (58:ef:68:b4:33:32) directly as a member of VLAN 10 (under Members by MAC Address), the switch dynamically maps that host to VLAN 10.
For any host dynamically matched via its MAC address, the FortiSwitch automatically handles the traffic on that port as untagged for that specific device.
upvoted 1 times

Clauster 3 months ago

Selected Answer: AD

The correct answers are A and D
A: When you add VLAN 10 as a member of the untagged this means this VLAN when Egress out of Port1 will send untagged traffic on VLAN10. When frames arrive on Port2 tagged for VLAN10 the switch assigns the frame VLAN 10, then it will see all of the ports that has VLAN 10 configured and forward traffic out of all those ports, Port1 will be untagged.
D: If you don't remove VLAN 10 from the Allowed list on Port 1 then all untagged Frames that PC1 sends will land on Native VLAN 20 causing the frames from PC1 to drop.
upvoted 1 times

Question #10 *Topic 1*

Which QoS mechanism maps packets with specific class of service (COS) or Differentiated Services Code Point (DSCP) markings to an egress queue?

A. Classification for ingress traffic

B. Queuing for egress traffic

C. Policing for ingress traffic

D. Shaping for egress traffic

Suggested Answer: *B*

Clauster 3 months ago

Selected Answer: A

Answer is A, here's the Fortinet documentation: https://docs.fortinet.com/document/fortiswitch/7.6.5/fortiswitchos-administration-guide/609009/classification

upvoted 1 times

79fad4e 3 months, 2 weeks ago

Selected Answer: A

Classification because fortiswitch maps packet with a given COS or DSCP page 266

upvoted 1 times

Question #11 *Topic 1*

What does the switch auto-network setting control on FortiSwitch?

A. The automatic VLAN assignment based on connected devices

B. The automatic discovery of the FortiGate->FortiLink interface

C. The root bridge priority for Multipl Spanning Tree Protocol (MSTP)

D. Whether the FortiSwitch can be managed by FortiManager

Suggested Answer: *B*

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

Question #12 *Topic 1*

Which statement best describes a benefit of using MAC, IP address, or protocol-based VLAN assignments on FortiSwitch?

A. It disables 802.1X authentication while preserving user access control.

B. It requires devices to authenticate through a RADIUS server before VLAN tagging.

C. It assigns ports to VLANs regardless of device type or traffic.

D. It offers dynamic segmentation benefits similar to 802.1X authentication.

Suggested Answer: *D*

SCC4exams 1 month, 1 week ago

Selected Answer: D

MAC, IP, and protocol-based VLANs on FortiSwitch provide benefits similar to those obtained when using 802.1X authentication.

This feature allows for dynamic assignment of ports to VLANs based on the characteristics of the incoming traffic, providing additional granularity in traffic segmentation and security. This is particularly beneficial in network environments that require precise control over device access without relying solely on standard 802.1X authentication.

upvoted 1 times

Question #13 *Topic 1*

Refer to the exhibit.

Debug output -

```
2025-07-23 12:13:19 573s:160ms:74us flp_event_handler[734]:node: port4
received event 101 state FL_STATE_WAIT_JOIN switchname S424DPTF20000029
flags 0x401
2025-07-23 12:13:21 575s:396ms:114us flp_event_handler[734]:node: port4
received event 110 state FL_STATE_READY switchname  flags 0x124a
2025-07-23 12:13:21 575s:398ms:724us flp_event_handler[734]:node: port4
received event 111 state FL_STATE_READY switchname  flags 0x124a
2025-07-23 12:13:21 575s:403ms:607us flp_send_pkt[445]:pkt-sent (type(5)
flag=0x18ca node(port4) sw(port4) len(26)smac: 0:50:56:96:d8: 2 dmac:
4:d5:90:c2:fa:ea
2025-07-23 12:13:22 576s:284ms:825us flp_send_pkt[445]:pkt-sent (type(3)
flag=0x8a node(port4) sw(S424DPTF20000029) len(26)smac: 0:50:56:96:d8: 2
dmac: 4:d5:90:c2:fb: b
2025-07-23 12:13:24 578s:411ms:316us flp_event_handler[734]:node: port4
received event 110 state FL_STATE_READY switchname  flags 0x124a
2025-07-23 12:13:24 578s:413ms:151us flp_event_handler[734]:node: port4
received event 111 state FL_STATE_READY switchname  flags 0x124a
2025-07-23 12:13:24 578s:415ms:255us flp_send_pkt[445]:pkt-sent (type(5)
flag=0x18ca node(port4) sw(port4) len(26)smac: 0:50:56:96:d8: 2 dmac:
4:d5:90:c2:fa:ea
```

Which two statements best describe what is displayed in the FortiLink debug output shown in the exhibit? (Choose two.)

A. FortiSwitch is in a waiting state to join the stack group on FortiGate.

B. FortiSwitch is sending FortiLink heartbeats to FortiGate.

C. FortiSwitch is discovered and authorized by FortiGate.

D. FortiSwitch is sending LLDP-MED inventory management updates to FortiGate.

Suggested Answer: *AB*

79fad4e 3 months, 2 weeks ago

Selected Answer: BC

B because it sends heardbeats to FortiGate and C because it says FL_STATE_READY

upvoted 1 times

Question #14 *Topic 1*

How does enabling an IGMP snooping proxy on FortiSwitch help reduce the number of IGMP reports processed by the IGMP querier?

A. By converting IGMP reports into broadcast packets to reach all VLAN members

B. By converting IGMP traffic to unicast

C. By suppressing duplicate IGMP reports within the VLAN

D. By forwarding IGMP reports only when the first member joins and the last member leaves

Suggested Answer: *D*

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

Question #15 *Topic 1*

How does FortiSwitch determine the route for traffic traversing its interfaces?

A. Hardware-based routing on FortiSwitch is handled by the CPU.

B. ASIC hardware routing can handle only dynamic routing, if supported.

C. FortiSwitch looks up the hardware routing table and then the forwarding information base (FIB).

D. FortiSwitch forwards all traffic to FortiGate for routing decisions.

Suggested Answer: *C*

SCC4exams 1 month, 3 weeks ago

Selected Answer: C

FortiSwitch determines the route for traffic traversing its interfaces by leveraging a two-tier routing lookup mechanism. It first checks the hardware routing table, which is populated with a subset of routes installed from the Forwarding Information Base (FIB) and programmed directly into the switch ASIC.

upvoted 1 times

Question #16 *Topic 1*

Refer to the exhibit.

FortiSwitch configuration -

```
# diagnose switch-controller switch-info loop-guard S108EF4N17000029
S108EF4N17000029:
  Portname            State     Status      Timeout(m)   MAC-Move   Count   Last-Event
  ________________    _______   _________   __________   ________   _____   ___________________
  port1               enabled   Triggered       2            0        1     2025-02-19 15:50:35
  port2               disabled  -               -            -        -          -
  port3               disabled  -               -            -        -          -
  port4               disabled  -               -            -        -          -
  port5               disabled  -               -            -        -          -
  port6               disabled  -               -            -        -          -
  port9               disabled  -               -            -        -          -
  port10              disabled  -               -            -        -          -
  8EF4N17000030-0     disabled  -               -            -        -          -
  _FlInK1_MLAG0_      disabled  -               -            -        -          -
```

You run the command diagnose switch-controller switch-info loopguard access-1 and see that the MAC-Move column displays a value of 0 for port1.

What does this indicate?

A. Loop guard is disabled on port1.

B. Port1 is not being monitored by loop guard.

C. The MAC move feature is not enabled.

D. Port1 will shut down if a loop occurs on any VLAN.

Suggested Answer: *C*

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

Question #17 *Topic 1*

A FortiGate is connected to a pair of FortiSwitch devices.
For redundancy, FortiGate must use uplinks on both switches simultaneously without depending on Spanning Tree Protocol (STP).
Which configuration is required?

A. Multi-tier topology

B. Multichassis link aggregation group (MCLAG)

C. Full mesh high availability (HA)

D. Link aggregation group (LAG)

Suggested Answer: *B*

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

Question #18 *Topic 1*

What is an advantage of using a FortiSwitch stack in managed switch mode with FortiGate when deploying VLANs?

A. FortiGate executing the routing and FortiSwitch managing its configuration.

B. Ensuring VLAN traffic can pass between connected switches in the stack.

C. FortiGate no longer needing to manage any VLAN configuration.

D. FortiGate provides visibility and control for inter-vlan traffic.

Suggested Answer: *D*

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

Question #19 *Topic 1*

What is one key advantage of using a sniffer profile on FortiSwitch compared to using the sniffer command?

A. It allows packet capture on all switch ports without limitations.

B. It eliminates the need to use access control lists (ACLs) or port mirroring for analysis.

C. It automatically filters irrelevant traffic types.

D. It automatically decrypts SSL/TLS traffic for full packet inspection.

Suggested Answer: *C*

SCC4exams 1 month, 1 week ago

Selected Answer: B

Correct answer is B

A sniffer profile on a FortiSwitch provides an easier and more flexible way to capture traffic compared to using the CLI sniffer command. It allows you to capture traffic directly on the switch interface without needing ACLs to filter traffic and Port mirroring (SPAN) configuration

upvoted 1 times

jeppe_rudolph 1 month, 1 week ago

Selected Answer: A

A - for sure. It's not comparing sniffer profile to ACLs, it's comparing sniffer profile and sniffer command.

Sniffer profile - Allows packet capture on every interface

Sniffer command - Allows packet capture on all interfaces but Trunks

upvoted 1 times

Cesaru888 1 month, 2 weeks ago

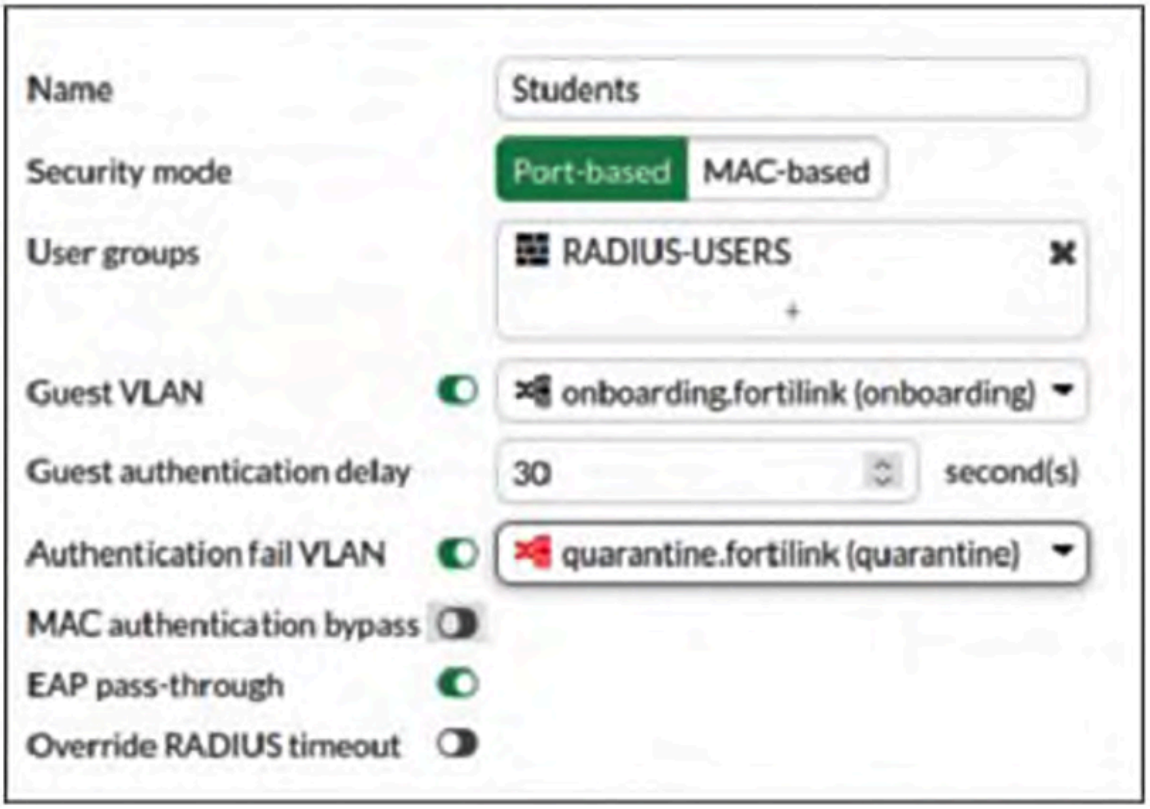
Selected Answer: B

B is true. The sniffer profile is a self-contained packet-capture method configured per switch port — you create the profile, start it, and download the capture straight from the FortiSwitch GUI. It captures the actual traffic on the port directly. The mirroring-based methods (SPAN/RSPAN/ERSPAN) work fundamentally differently: they copy a port's traffic to a destination interface where a separate monitoring device captures it, and to filter that mirrored traffic you must configure an ACL classifier and reference the SPAN profile. The sniffer profile avoids that whole apparatus — no port mirroring to a destination, and no ACL classifier needed to scope the capture — which is its key advantage over the limited sniffer command (which on switch ports captures only certain packet types like ingress LLDP and BPDUs).

upvoted 1 times

Question #20 *Topic 1*

Refer to the exhibit.



The security port policy is configured as shown in the exhibit.
Which behavior occurs if a device connected to the port that does not support 802.1X?

A. The device is blocked from accessing the network.

B. The device is placed into the onboarding VLAN.

C. The device is placed into the quarantine VLAN.

D. The device is assigned to the default management VLAN.

Suggested Answer: *B*

giutiz 1 month, 2 weeks ago

Selected Answer: B

With port-based 802.1X enabled and a guest VLAN configured, devices that do not support or do not complete 802.1X authentication are automatically placed into the guest (onboarding) VLAN, allowing limited or remediation access instead of being fully blocked or quarantined.

upvoted 1 times

Question #21 *Topic 1*

When Dynamic Host Configuration Protocol (DHCP) snooping is enabled on a FortiSwitch VLAN, which two statements are true? (Choose two.)

A. DHCP replies are accepted only on trusted ports.

B. DHCP snooping blocks all unicast traffic.

C. Option 82 can be inserted into DHCP requests.

D. DHCP requests are dropped if sent from trusted ports.

Suggested Answer: *AC*

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

Question #22 *Topic 1*

Refer to the exhibit.

Debug capture of the fortilinkd process on FortiGate

```
FGT-1 # diagnose debug application fortilinkd 3
Debug messages will be on for 30 minutes.
 ......
133s:933ms:828us flp_get_rx_node[179]:received hdr_type(4) reserved(0x194) portname(port4) swnode(FS24VMTM25000128) fsw(FS24VMTM25000128)
133s:945ms:945us flp_get_rx_node[179]:received hdr_type(6) reserved(0x194) portname(port4) swnode(FS24VMTM25000128) fsw(FS24VMTM25000128)
133s:959ms:628us flp_event_handler[767]:node: port4 received event 110 state FL_STATE_WAIT_CONN switchname FS24VMTM25000128 flags 0x1
133s:971ms:684us flp_get_rx_node[179]:received hdr_type(6) reserved(0x194) portname(port4) swnode(FS24VMTM25000128) fsw(FS24VMTM25000128)
133s:985ms:693us flp_event_handler[767]:node: port4 received event 112 state FL_STATE_WAIT_CONN switchname FS24VMTM25000128 flags 0x1
 ......
341s:88ms:941us flp_get_rx_node[179]:received hdr_type(6) reserved(0x194) portname(port4) swnode(FS24VMTM25000128) fsw(FS24VMTM25000128)
341s:102ms:437us flp_get_rx_node[179]:received hdr_type(4) reserved(0x194) portname(port4) swnode(FS24VMTM25000128) fsw(FS24VMTM25000128)
341s:114ms:586us flp_get_rx_node[179]:received hdr_type(4) reserved(0x190) portname(port4) swnode(FS24VMTM25000129) fsw(FS24VMTM25000129)
341s:125ms:871us flp_event_handler[767]:node: port4 received event 110 state FL_STATE_READY switchname FS24VMTM25000128 flags 0x401
341s:140ms:645us flp_event_handler[767]:node: port4 received event 110 state FL_STATE_READY switchname FS24VMTM25000129 flags 0x401
341s:151ms:123us flp_event_handler[767]:node: port4 received event 111 state FL_STATE_READY switchname FS24VMTM25000128 flags 0x401
341s:163ms:741us flp_send_pkt[469]:pkt-sent (type(5) flag=0xca node(port4) sw(FS24VMTM25000128) len(26)smac: 2: 9: f: 0: 5: 1 dmac:36:1c:17:b2:5e:be
```

A periodic heartbeat message sent from a managed FortiSwitch and corresponding acknowledgments from FortiGate is shown.

What does this behavior indicate?

A. The FortiLink connection between FortiGate and FortiSwitch is healthy and active.

B. FortiGate is unable to establish a FortiLink session with FortiSwitch.

C. ForitSwitch is expecting an authorization from FortiGate.

D. FortiSwitch has not been authorized yet.

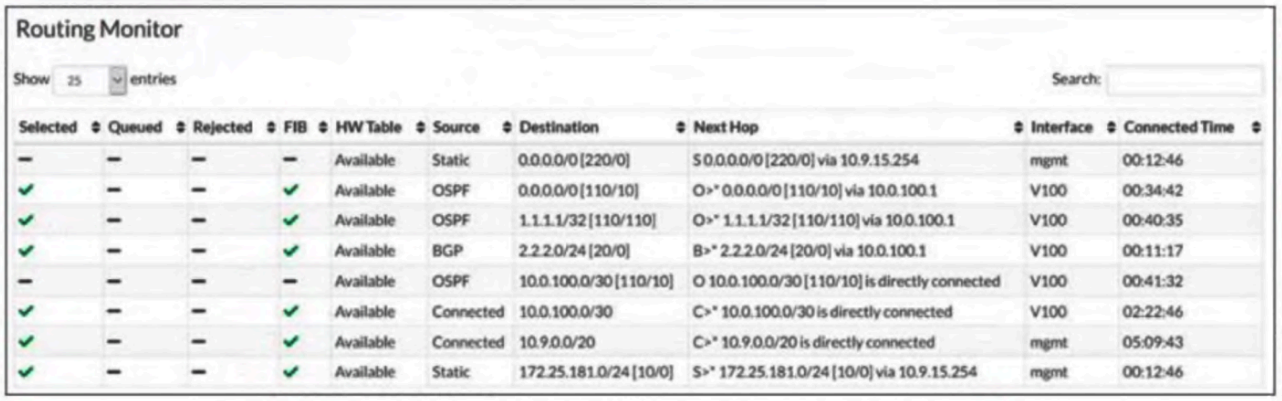
Suggested Answer: *A*

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

Question #23 *Topic 1*

Refer to the exhibit.

Routing Monitor -



Routing Monitor

Show 25 entries Search:

Selected	Queued	Rejected	FIB	HW Table	Source	Destination	Next Hop	Interface	Connected Time
–	–	–	–	Available	Static	0.0.0.0/0 [220/0]	S 0.0.0.0/0 [220/0] via 10.9.15.254	mgmt	00:12:46
✔	–	–	✔	Available	OSPF	0.0.0.0/0 [110/10]	O>* 0.0.0.0/0 [110/10] via 10.0.100.1	V100	00:34:42
✔	–	–	✔	Available	OSPF	1.1.1.1/32 [110/110]	O>* 1.1.1.1/32 [110/110] via 10.0.100.1	V100	00:40:35
✔	–	–	✔	Available	BGP	2.2.2.0/24 [20/0]	B>* 2.2.2.0/24 [20/0] via 10.0.100.1	V100	00:11:17
–	–	–	–	Available	OSPF	10.0.100.0/30 [110/10]	O 10.0.100.0/30 [110/10] is directly connected	V100	00:41:32
✔	–	–	✔	Available	Connected	10.0.100.0/30	C>* 10.0.100.0/30 is directly connected	V100	02:22:46
✔	–	–	✔	Available	Connected	10.9.0.0/20	C>* 10.9.0.0/20 is directly connected	mgmt	05:09:43
✔	–	–	✔	Available	Static	172.25.181.0/24 [10/0]	S>* 172.25.181.0/24 [10/0] via 10.9.15.254	mgmt	00:12:46

The routing monitor displays multiple route entries, but only some are installed in the forwarding information base (FIB).
After analyzing the two route entries with the destination 0.0.0.0/0, which statement correctly describe why one of these routes is not installed in the FIB?

A. The OSPF route has a higher metric, making it less preferred than the static route.

B. The interface V100 for the OSPF route is down, preventing its installation.

C. The OSPF route with a lower administrative distance is preferred over the static route.

D. The two routes have identical destination prefixes, causing a conflict where only one is selected.

Suggested Answer: *C*

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

Question #24 *Topic 1*

You are deploying a small office network with a single FortiGate and a single FortiSwitch. The office currently has moderate traffic, but the IT team expects the network to grow in the near future, adding more FortiSwitch devices and endpoints.
Which FortiLink configuration should you deploy to provide the best combination of current performance and scalability for future growth?

A. Configure FortiLink using hardware-based switch interfaces.

B. Configure FortiLink using software-based switch interfaces.

C. Configure FortiLink as a link aggregation group (LAG) interface.

D. Configure FortiLink as a multichassis LAG (MCLAG) interface.

Suggested Answer: *C*

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

Question #25 *Topic 1*

You are configuring VLANs on a FortiSwitch device managed by FortiGate.
Which two statements accurately describe VLAN assignment requirements and behavior on FortiSwitch ports? (Choose two.)

A. Untagged defines the list of VLANs that are allowed on the port for both ingress and egress traffic.

B. Untagged VLAN applies to egress traffic only.

C. You can assign only one native VLAN on a port.

D. VLAN assignments must be configured directly on the FortiSwitch.

Suggested Answer: *BC*

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

Question #26 *Topic 1*

You are configuring FortiSwitch to perform layer 3 inter-VLAN routing while managed by FortiGate over FortiLink. On supported hardware models, FortiSwitch can offload routing decisions for better performance.
How does FortiSwitch perform routing between VLANs?

A. By using a hardware forwarding table (FIB) programmed into ASIC.

B. By supporting only dynamic routing protocols in hardware.

C. By disabling routing when managed by FortiGate.

D. By relying entirely on the CPU in software.

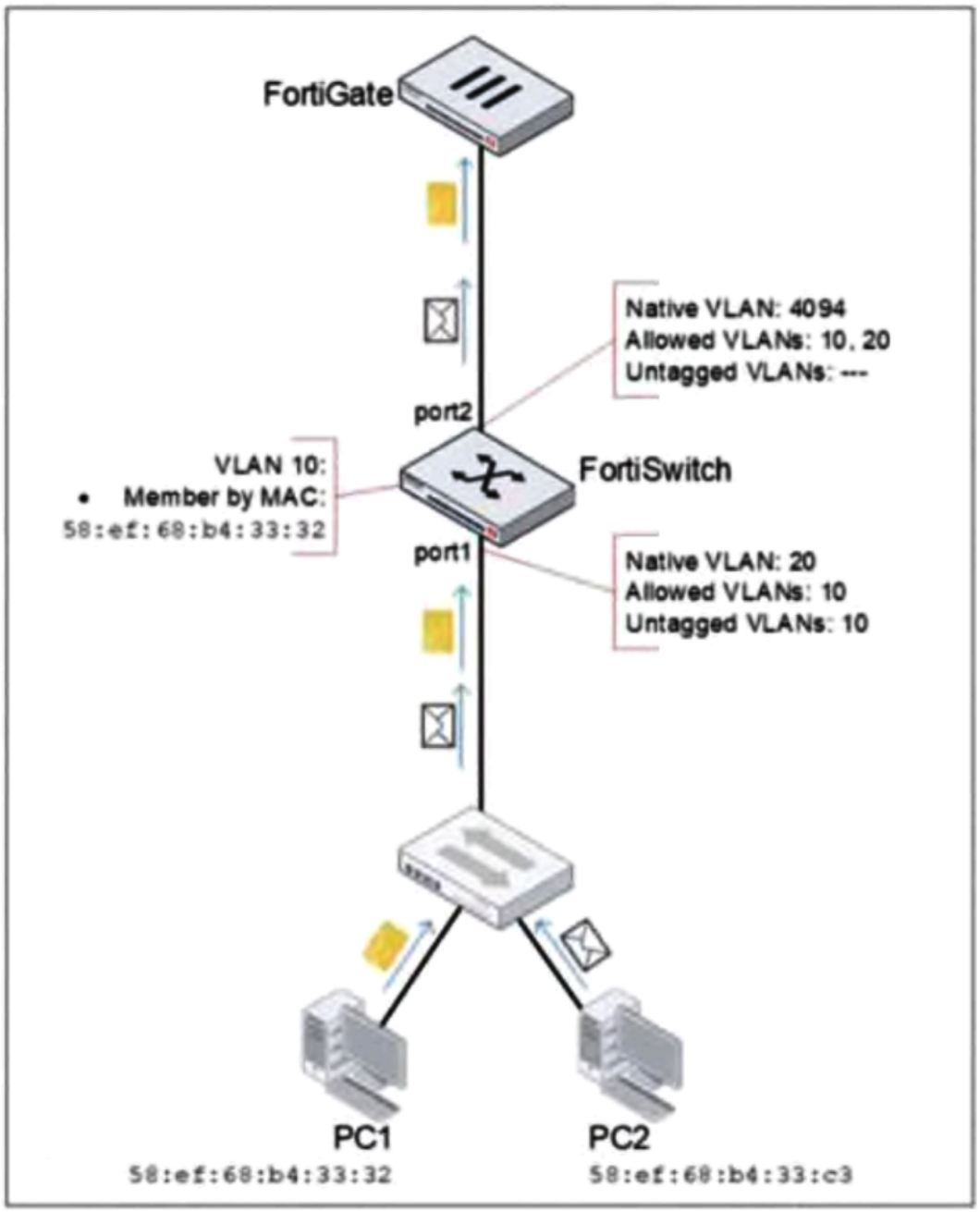
Suggested Answer: *A*

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

Question #27 *Topic 1*

Refer to the exhibit.

Network Topology -



PC1 and PC2 are connected to port1 on FortiSwitch.
Which VLAN tags will FortiSwitch apply when forwarding PC1 and PC2 traffic out of port2?

A. FortiSwitch will tag PC1 and PC2 frames with VLAN 20.

B. FortiSwitch will tag both PC1 and PC2 frames with VLAN 10, due to MAC override.

C. FortiSwith will tag PC1 frames with VLAN 10 and PC2 frames with VLAN 20.

D. FortiSwitch will leave PC1 frames untagged and will tag PC2 frames with VLAN 10.

Suggested Answer: *C*

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

Question #28 *Topic 1*

You are deploying a FortiSwitch virtual stack in a network that contains Cisco devices. You want the Cisco devices to automatically discover the FortiSwitch devices and exchange device information.
Which two protocols must be enabled on the FortiSwitch devices to achieve this? (Choose two.)

A. Unidirectional Link Detection

B. Cisco Discovery Protocol

C. Link Layer Discovery Protocol

D. LLDP - Media Endpoint Discovery

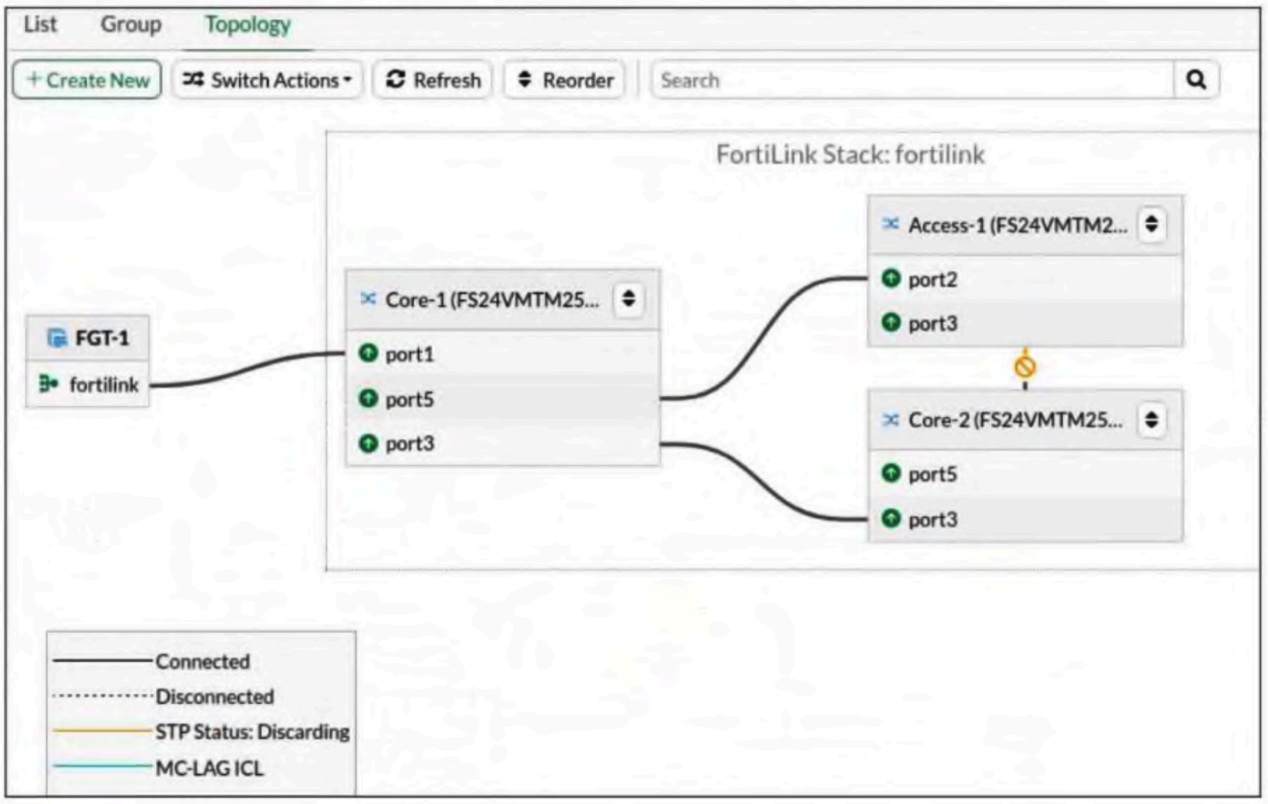
Suggested Answer: *BC*

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

Question #29 *Topic 1*

Refer to the exhibit.

Topology view -



You just connected three FortiSwitch devices: Core-1, Core-2, and Access-1. Core-1 and Core-2 both connect to Access-1 for redundancy.
All switches are managed by FortiGate, which uses port4 as the FortiLink interface. After you enable the uplink ports on Core-2, you notice that port3 on Access-1 enters the Discarding STP state.
What is the most likely cause of this behavior?

A. Bridge Protocol Data Unit (BPDU) Guard is enabled, which shuts down the port after it receives BPDUs.

B. Access-1 is not authorized by FortiGate.

C. Core-2 has the lowest bridge priority.

D. FortiGate is not running Spanning Tree Protocol (STP) on the FortiLink interface.

Suggested Answer: *D*

Clauster 3 months ago

Selected Answer: C

C: Access-1 sees that Core-2 has a lower Bridge ID which will cause the link between them to negotiate, it will place it's port 1 to Discarding while Core-2 will set his port to Designated. This is typical STP behavior.
It can't be D.
upvoted 1 times

Question #30 *Topic 1*

When you change FortiSwitch management mode from standalone to managed, what happens to the existing standalone configuration?

A. FortiSwitch registers to FortiSwitch Cloud to save a copy before managing with FortiGate.

B. FortiSwitch merges the existing standalone configuration with the default FortiLink configuration.

C. FortiSwitch saves the standalone configuration and changes to the default FortiLink configuration.

D. FortiGate automatically saves the existing FortiSwitch configuration during the FortiLink management process.

Suggested Answer: *C*

f2ed534 1 month ago

Selected Answer: C

According to the official NSE 5 FortiSwitch 7.6 Study Guide (and the FortiLink Auto-Discovery process documentation), the correct answer is:

C. FortiSwitch saves the standalone configuration and changes to the default FortiLink configuration.

upvoted 1 times

Question #31 *Topic 1*

Refer to the exhibit.

Commands -

```
config switch-controller lldp-profile
    edit "Phone"
        set med-tlvs network-policy
        set auto-isl disable
        config med-network-policy
            edit "voice"
                set status enable
                set vlan-intf "voice"
                set assign-vlan enable
                set dscp 46
            next
            edit "voice-signaling"
                set status enable
                set vlan-intf "voice"
            next
            edit "guest-voice"
            next
            edit "guest-voice-signaling"
            next
            edit "softphone-voice"
            next
            edit "video-conferencing"
            next
            edit "streaming-video"
            next
            edit "video-signaling"
            next
        end
    next
end
```

The LLDP profile shown in the exhibit was configured to detect IP phones and automatically assign them to the appropriate VLAN. You apply this LLDP profile on a FortiSwitch port.
Which configuration should you enable on the FortiSwitch profile to collect detailed information about all the connected IP phones?

A. Create a new LLDP profile to handle different LLDP-MED TLVs.

B. Configure a dedicated voice VLAN with DSCP 46.

C. Enable LLDP-MED inventory management TLVs.

D. Enable auto-isl.

Suggested Answer: *C*