MILKATURKA

Business Background

MilkaTurka is a well known company which produces daily fresh milk, five different kinds of cheese and the any other milk products.

Company is founded in 1986 and the over the years business growth very rapidly.

Their all operation is located throughout Turkey. They have 480 front stores, which they sell their products and they operate, in 45 different cities in the Turkey.

In each city they have at least one production facility, which provides all the products to the stores in the same city.

In Istanbul, Ankara and Izmir they have at least 20 stores and all these 3 cities they have two production facilities.

Their HeadQuarter is located in the Istanbul. They have a mid range datacenter in the HeadQuarter building which hosts servers, store and production facility connections, network security devices including Firewalls, IPS/IDS, Load Balancers and the Proxies.

They don't have so many applications and the important ones for the business are Voice over IP, ERP application which they manage the stocks, pricing information and the sales data and an email.

They have two datacenters, one of them in the Istanbul HeadQuarter as it is stated above and the one in Izmir.

They are using Izmir data center as a Disaster Recovery facility since their none of the application require less than 10 minutes convergence time. They considered to build active-active datacenter last year but the CAPEX and OPEX of building active-active datacenter was too costly for them.
In the Istanbul Headquarter there are 21 Vlans , 10 for the data and 10 for the voice and 1 vlan is allocated to the wireless network.

In the stores there are only three vlans. One for the general data usage, One for the IP phones and One for the computers, which has an access to the ERP application. The store manager can only control this computer.

Currently they don't have any quality of service (QoS) in their network.

In their last board meeting MILKATURKA decided to sell some of their products at 1400 SASA locations. They know that this will cause a lot of business and technical challenges to them.

SASA

Business Background

SASA is the biggest hypermarket chain in the Turkey. They have 3200 stores in Turkey and 1400 of them are close enough to MILKATURKA locations, that's why MILKATURKA will only sell their products at those 1400 stores.

SASA has many suppliers similar to MILKATURKA and they provide a shelve in their market to the suppliers.

SASA has two types of markets; SASA and SASA mini. In the SASA stores there are around 60 personnel including store managers, deputy managers , cashiers and the rest.

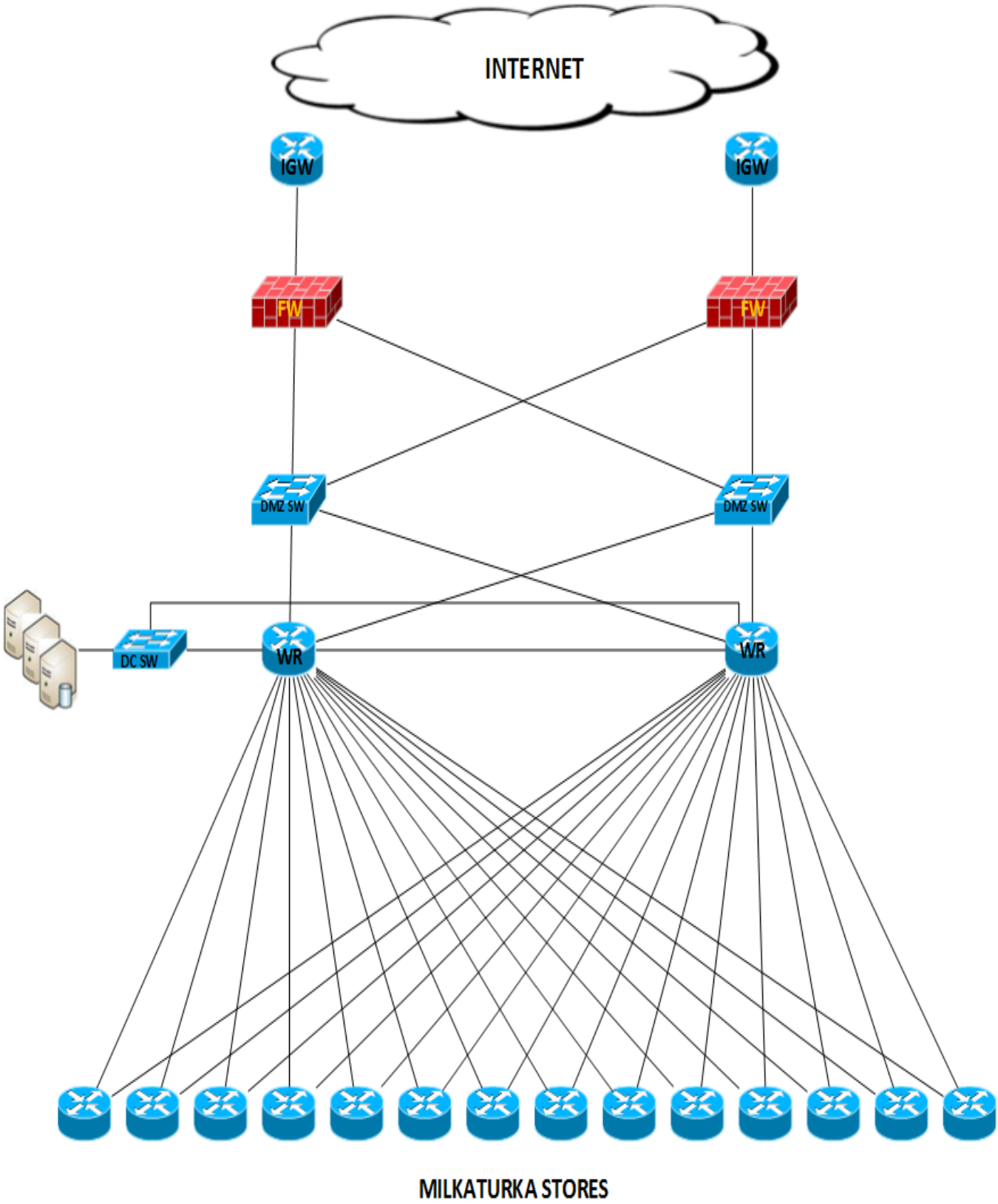
In SASA mini they usually have 6 or 7 personnel since the size of the SASA mini stores are very small.

In each SASA store, there is local PC which keeps the sales and stock information.

All SASA stores are connected to SASA Datacenter and the stock inventory is uploaded to the central servers weekly.
If the product price needs to be updated, changes are reflected immediately from the server to the stores at the same time.
Problem with the weekly update for the MILKATURKA and other many suppliers, their products might be out of stock and they couldn't be informed until they receive weekly update.

Thus, MILKATURKA wants to have the stock information as close to real time as possible. Application at each store which will provide real time sales and stock data, only running IPv6 and this is going to be another challenge for MILKATURKA since their network currently doesn't support IPv6.

NETWORK DIAGRAMS



Question 1 : What are the main concerns of MILKATURKA based on provided information ? (Choose all that apply)

A – Installing and operating new circuits/connections to provide connectivity between MILKATURKA DC and each SASA store.

B- To find an equipment which can support the connectivity requirements.

C- Purchasing the physical hardware, router/firewall to provide connectivity to each SASA store.

D- Securing the connections required to provide connectivity to each store.

Answer 1 : This question is looking to analyze the design requirements. Candidate should be able to understand where the complexity can be in this type of design.

Answer is Option A and Option D. Detail explanation for the reason will be provided in Answer 2 and Answer 3.

Question 2 : Why do you think installing and managing the new circuits is difficult ?

A- Large scale connectivity requirement brings operational complexity

B – Configuring the thousands of devices will be difficult

C- During configuration of thousands of devices, many configurational mistakes can be made

D- Number of head end devices to support additional connections at the MILKATURKA DC

Answer 2 : We know that this scale of design bring operational complexity, managing the VPN/Tunnel connections, managing the

routing protocol which might be required will bring operational complexity.

But even though thousands of SASA devices need to be configured, automated provisioning tools can be used to minimize the configurational error and reduces the required time for provisioning greatly. That's why Option B and Option C are incorrect.

Since we haven't determined the connection type and whether additional device will be used at the MILKATURKA DC for the new connections, option D is wrong as well. MILKATURKA might use existing routers/firewalls to support the new connections.

Only correct answer is Option A for this question. This is analyzing the questions part in the exam and in general candidates fail because of this part.

Question 3 : What is the first security problem based on the information given so far, from the MILKATURKA point of view ?

A- The new MILKATURKA equipment which will be installed to every SASA store to support new connections, physically outside the control of MILKATURKA

B- Number of security polices will be too much since the number of devices which MILKATURKA install at the SASA stores.

C- Firewalls at the SASA stores may not support IPSEC encryption

D- Routers at the SASA stores may not support IPSEC encryption

E- All options are correct

ANSWER 3 :

Option A is correct because whichever solutions are chosen, installing new hardware, firewall/routers and so on or using tunnels on the existing SASA devices will be outside the control of MILKATURKA

Although numbers of devices or tunnels are going to be too much, it doesn't mean number of security policies will be too much as well. Instead for the modular design, one common security policy should be applied to each store by the MILKATURKA. That's why Option B is incorrect.

We don't know there is firewall or router and even whether they will allow to use to those or MILKATURKA security team is going to use those. That's why Option C ad Option D are incorrect.

Since the correct answer is Option A, Option E is incorrect.

QUESTION 4 : Which below options are required to start the design based on the provided information so far ? (choose two)

A- Number of SASA location which MILKATURKA is going to sell their products.

B – Amount of traffic the SASA ERP application that will send the sales and stock data to the MILKATURKA

C - Typical network configuration of the SASA stores

D- Security level requirements of the MILKATURKA stock and sales data

E- All of the above

Answer 4 :

With this type of question, exam is looking whether you can ask the right information to start working on the design. You shouldn't make assumptions. Otherwise you will fail.

In the CCDE exam if information is already provided to you, you cannot ask it again. This is true also for real life design. If your customer already provided you information, you don't ask the same information again.

Number of location which MILKATURKA will sell their products are 1400; this information has been given to you in the beginning. That's why Option A is incorrect.

ERP applications don't create enough information to impact the design significantly. Also at this point we should first determine whether the existing SASA equipment will be used or new equipment needs to be installed at every SASA store or tunnels will be selected. Application speed and feed doesn't change the design decisions. But this doesn't mean application requirements don't impact design decisions. Just at his point speed requirement is not important.
That's why Option B is incorrect.

Without knowing typical network configuration of SASA stores, MILKATURKA cannot decide whether they need new circuit or they can create a tunnel to the existing devices and so on. That's why Option C is correct and important.

Sales and Stock data which is required by MILKATURKA may not critical from the security point of view. SASA and MILKATURKA should provide the required protection level for the data and this information is important and haven't provided yet. Option D is correct as well.

EMAIL 1 is Available

Hi MILKATURKA,

Please be informed that we are okay with putting your additional device and link if you need, but required extra power on 1400 locations our concern. You should talk this with the upper management.
Our device is capable to provide a tunnels. Let's work on this to find the best solution for you.

Question 5 : Do you recommend MILKATURKA to install a new equipment and circuit into each SASA store ?

A- YES
B – NO

Answer 5 :

No. Detail Answer will be provided in Answer 6.

Question 6 : What would be the alternate design if you don't install new equipment and new circuit ?

A – Configure a tunnel on the existing SASA devices

B- Rely on weekly report which will be provided by the SASA

C- Purchase only new circuit on each SASA store and connect on existing SASA equipment

Answer 6 : In this type of design, new device and new link always comes to network engineer's mind first.

But the problem at this scale is not the CAPEX. Purchasing the new device and new link although initially might be costly, actual cost comes from the OPEX site.

Managing the devices, when something fails or faulty, sending a technician to the site, replacing the equipment, opening a ticket to the vendor, or to the ISP, required extra power, cooling etc. for the new equipments all are the operational expenses.

Alternate solution always should be considered by the network engineers/designers without doing assumptions.

In the Email-1, SASA networking team already said that if MILKATURKA needs tunneling solutions to their equipment, their devices are capable and SASA is willing to help.

That's why Question 5's answer is NO since we have much better solution for this network design.

Since in the business information it is given that MILKATURKA doesn't want to rely on weekly report, which will be provided by the SASA, you cannot choose option B.

Also tunneling by using existing SASA equipment and the circuit is much better operationally than purchasing new 1400 circuits even though they allow to provide a port on their equipment.

Question 7 : MILKATURKA decided to create a tunnel instead of relying on weekly update or purchasing new circuit, to connect to SASA equipment.

What do you need to decide which tunneling solution to be used ?

A - What are the security requirements for the sales and stock data ?

B - Network convergence time requirement for the application

C- Which type of transport application requires, Layer 2 or Layer 3 ?

D- All of the above

Answer 7 : You need to know what are the security requirements such as; Do you need encryption?

How important the data security?

Because some tunneling technologies can scale better without encryption, some comes with security, some without. This is very important to decide tunneling technology to be used.

It is already given in the beginning of the scenario that MILKATURKA's application convergence requirement is not tight. Even though 10 minutes time is totally okay, so convergence time is not critical for this design.

Application transport requirement is always important to decide tunneling technology. Some tunneling technologies doesn't support layer 3 , some of them don't support layer 2. But in the beginning of the scenario it is given that application is running on

IPv6. We need a tunneling mechanism which can support IPv6 traffic (Layer3)

We should know the transport requirement as well.
That's why answer of this question is Option A.

Question 8 : For each of the tunneling technologies in the below chart, please mark the areas that would be a concern for the MILKATURKA.

	uration and Management xity	e Over Public WAN
2 VPN		
3 VPN		
nnels		
unnels		

Answer 8 : We need to understand the capabilities of the tunneling technologies in the above chart.

We are looking for the tunneling types, which can support IPv6, since the application require IPv6 support.

Mpls L2 VPN : MPLS L2 VPN cannot be an option because, the tunnels will be created over the Public Internet connections of MILKATURKA and SASA.

MPLS L3 VPN: MPLS L3 VPN cannot be an option because, the tunnels will be created over the Public Internet connections of MILKATURKA and SASA.

GRE: Configuration and the management of the GRE tunnels are overkill. Especially in this type of large scale deployment. If it used with mGRE technology or with DMVPN architecture then the configuration and management requirement could be reduced greatly.

Service provider sees IPv4 packets only. GRE traffic is not a concern. Service Provider can block the GRE traffic if they want but they don't. in general. Service Provider to Service Provider peering location is exceptional since there are some attack types over BGP peering. It is very suitable over Public WAN.

IPSEC: Creating IPSEC tunnels same as GRE , it is overkill, since the Security Association is created between each end points. If it is used with the technology, which can support multipoint to multipoint Security Association such as GETVPN, then configuration and management requirement can be reduced greatly.

IPSEC traffic is also seen as IP traffic by the service provider, so it is not a concern as well. It is suitable technology over public Wide

	uration and Management exity	e over Public WAN
2 VPN		
3 VPN		
nnels		
Tunnels		

Area Networks.

That's why the answer for the question 8 is as above.

Question 9: Which tunneling technology would you recommend for the connection between MILKATURKA and the SASA stores?

A- MPLS L2 VPN

B- MPLS L3 VPN

C- GRE

D- IPSEC

E- VPLS

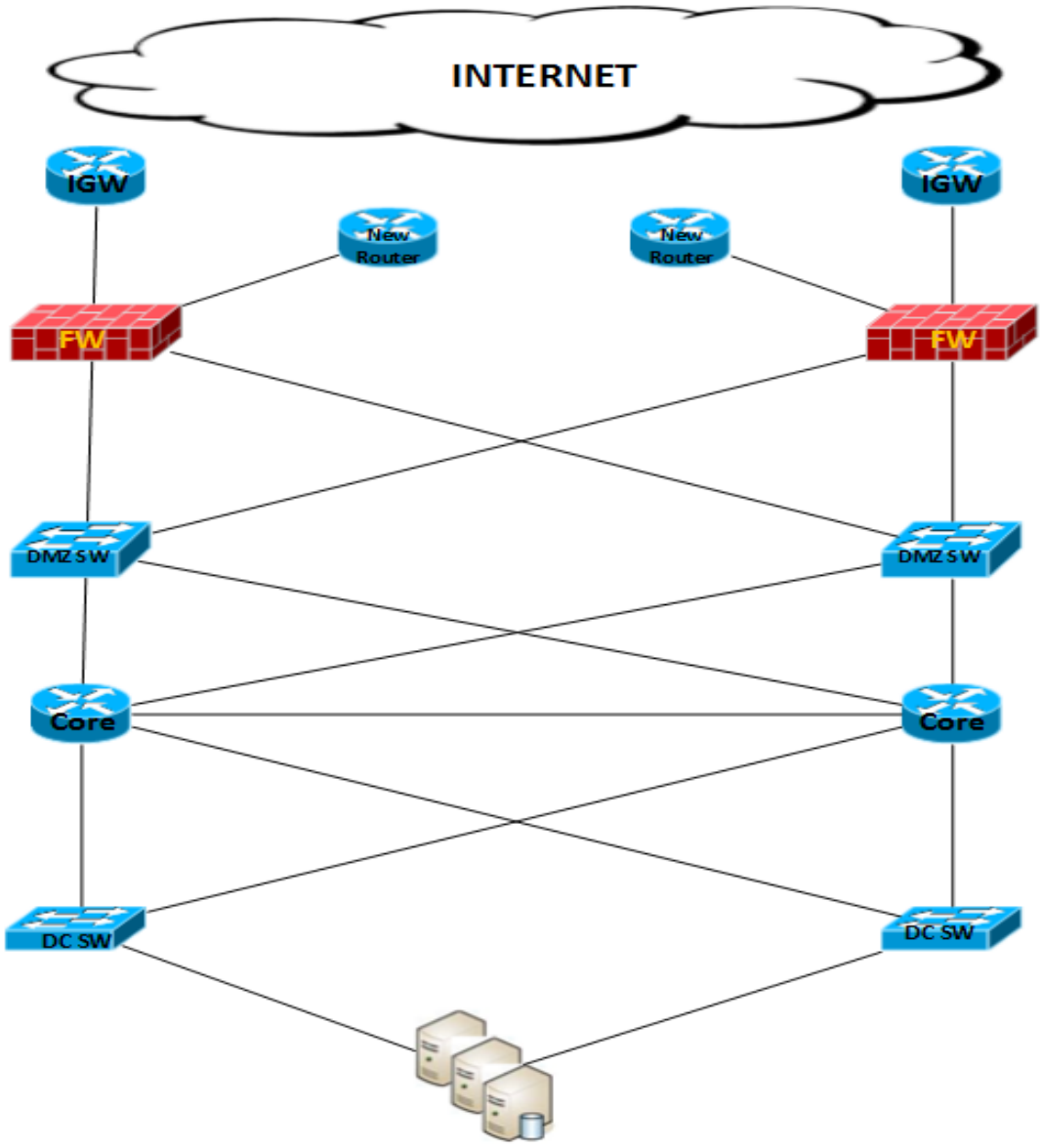
Answer 9 : As it is indicated earlier MPLS L2 and MPLS L3 VPN cannot run over the Public WAN. They could be an option if the private circuit would be purchased in the first place.

Although GRE tunnels are operationally complex from the configuration and management point of view, it supports IPv6 among the given options.

IPSEC would be an option but since there is no encryption requirement as it is indicated in the email, it is not selected since it puts a lot of extra burden compare to all the other tunneling option on the hardware.

Correct answer for this question is GRE, which is Option C.

Question 10: Based on the below diagram of MILKATURKA, where would you deploy the GRE tunnels?



A – Existing core router should be used to bring the GRE tunnels.

B-GRE tunnels should be terminated on the DC Switches so traffic is hand off to the closest point to the servers

C-New router should be purchased and connected to the firewalls and GRE tunnels should be terminated on this new router

D-Existing Internet Gateway routers should be used for the GRE tunnels

E-Any of this place is actually same for the MILKATURKA network design

Answer 10: If GRE tunnels are terminated on the existing core routers or the newly purchased router which is connected to the network core, firewall cannot inspect the traffic and untrusted traffic directly comes to the internal network.

If GRE tunnels would be terminated on the DC switches similar think would happen with the terminating GRE tunnels on the existing Network core routers.. Firewall cannot inspect the traffic and untrusted traffic would be brought to the internal network.

From the security point of view this is a treat. That's why Option A and Option B are invalid options.

Also bringing GRE traffic directly to the network core routers mean, if something fails in the SASA store network, will impact the core routers of Milkaturka. We know that SASA equipment is not in MILKATURKA's control.

By purchasing new router and connecting it to the network core routers or to the firewalls, failure domain separation is achieved but connecting new router to the network core means, untrusted traffic is brought to the internal network as it is explained above as well.

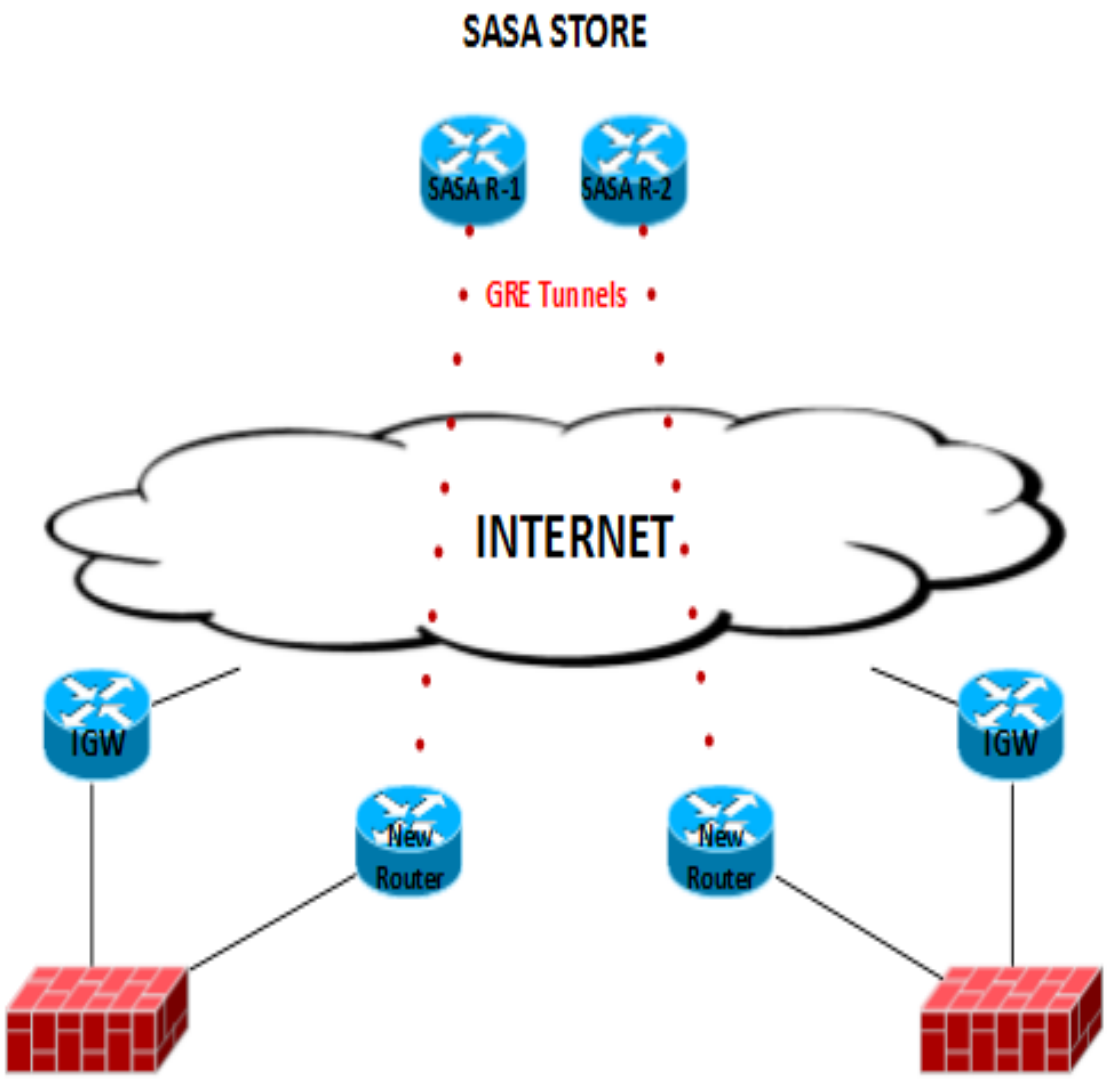
Using existing equipments always mean fate sharing. Terminating GRE on the core routers or on the Internet gateways.

In that case, instability in the SASA stores will affect the Internet Gateway or Network core routers, which is definitely unwanted.

Correct solution is to purchase new equipment so provide failure domain separation and connect the newly purchased router behind the firewall so stateful packet inspection can be done after decapsulating GRE traffic since it has to go through firewall.

That's why Option C is the correct answer.

Question 11 : MILKATURKA network architect proposed the below tunnel configuration. Do you think the proposed tunnel design is best for the MILKATURKA ?



A- Yes
B- No

Answer 11 : No it is not. The detail answer will be provided in Answer 12.

Question 12 : Why you don't agree with the proposed tunnel design ?

A- There should be only one GRE tunnels per SASA store

B- GRE tunnels shouldn't pass through the firewalls

C- GRE tunnels should be terminated on the Internet Gateways

D- There should be four GRE tunnels per SASA store

E- GRE tunnels should terminate on the firewalls

Answer 12 : GRE tunnels should be terminated behind firewalls as it is explained in the Answer 10. Incoming traffic first will go through as GRE, but then it is terminated on the router behind the firewall. That's why Option B is wrong.

It will not be terminated on the firewall or Internet gateways. That's why Option C and Option E are wrong.

Should be only one or only four tunnels per SASA stores ?

As it is given in the business information at the beginning of the scenario, application is not critical from the convergence point of view.
The tradeoff is the convergence vs. number of tunnels. Having one extra tunnel per store mean, 1400 extra tunnels overall.

Since application doesn't require fast convergence, having 1400 extra tunnel is overkill. Also having second tunnel on the different router only protects the router failure, which is not so common failure.
That's why answer of this question is to have only one GRE tunnel per SASA store, which is Option A.

Question 13 : Which type of network WAN topology is the new tunnels between MILKATURKA and the SASA stores ?

A- Partial Mesh

B- Full mesh

C- Ring

D- Hub and Spoke

E- Square

Answer 13 : Since there is no store to store requirement is given and all the store is connected to the MILKATURKA DC, this topology is called Hub and Spoke.

If the requirement would be to connect some SASA store directly through the tunnels, topology would be Partial Mesh , and if the requirement would be to connect every store directly to each other (Such as DMVPN) then the topology would be Full mesh.

The correct answer for this question is Hub and Spoke which is Option D.

Question 14: Which routing protocol MILKATURKA should run over the new Hub and Spoke tunnel network to support Scalability and the other given requirements ?

A- OSPFv2

B- EIGRP

C- OSPFv3

D- IS-IS

Answer 14 : SASA store as it is given at the beginning, is running IPv6. Since the application traffic over the GRE tunnels are going to be carried as IPv6, overlay protocol should support IPv6.

As we know, OSPFv2 doesn't support IPv6. Among all the options, only OSPFv2 cannot carry IPv6 traffic

Also, as we know we need at least 1400 store tunnels , this mean having minimum 1400 at the routing table, building and maintaining 1400 routing adjacency at the MILKATURKA HUB site.

Although it is not asked in the scenario so far, if in the future second tunnel is added per site, scalability demand grows.

In order to provide current and future scalability requirement, EIGRP should be selected among the given routing protocols.

The correct answer is EIGRP which is Option B.

Question 15 : Which one would be the important design problem for the tunneled WAN network ?

A- Quality of Service configuration required to support Routing Protocol

B- Number of route in the routing table

C- Number of routing protocol adjacency

D- Packet replication which can cause packet drop at the HUB site

E- Security configuration between the routing neighbors create configuration complexity

Answer 15 : Quality of service is not related with the routing protocol. The customer should give whether or not the Quality of Service is required. Also so far there is no obvious Quality of Service requirement is seen in the scenario.

Application network from the stores will be kept on the MILKATURKA Hub site, which mean 1400 route in the routing table. This amount of route is supported all the modern routing platform. This is not an issue either.

The problem comes from the number of routing adjacency. Supporting 1400 EIGRP adjacency on the routing platform is an

engineering issue and can be the important design problem with this scale requirement.

Packet replication is done for the multicast packets but routing protocol packets are not replicated so this is not en issue either.

There is no routing protocol security requirement but even though it would be given, it is not a routing problem.

That's why the answer is Number of routing protocol adjacency which is Option C.

Question 16 : How many routers should MILKATURKA install at the DC to terminate all the tunnels from SASA stores ?

A- One

B- Two

C- Three

D- Four

E- It depends

Answer 16 : As it is explained in the Answer 15, the problem is the number of routing protocol adjacency. It is not the only consideration to understand how many routers is needed to terminate spoke tunnels.

As it is decided, GRE Tunnels will be terminated at the MILKATURKA Hub routers.

GRE encapsulation and decapsulation should be done on special hardware on the routers.

There is no enough information about the router hardware, if it supports GRE on the hardware, how many EIGRP protocol neighborship can be supported and so on.

This question is looking whether you will do the assumption and choose the two for redundancy.

The correct answer is it depends which is Option E because more information should be provided.

Question 17 : Which routing protocol feature should be enabled at the store site ?

A- OSPF Stub Area

B- BFD

C- EIGRP Stub

D- EIGRP Feasible Successor

E- EIGRP NSSA Area

Answer 17 : Since in the earlier question we know that EIGRP is suitable for the new tunneled WAN network, OSPF features , OSPF Stub and OSPF NSSA Area is not correct.

We also know that there is no fast convergence requirement. In fact even 10 minutes convergence time is okay and all the routing protocol even with the default timers can convergence quicker than 10 minutes. BFD is used for the fast failure detection and no need in this network. Thus Option B is incorrect too.

EIGRP feasible successor is very important EIGRP feature, which provides the loop free backup path. Backup path is calculated and

installed in the EIGRP topology table, which provides faster convergence time, compare to other routing protocols default convergence time. But for this network it is irrelevant since we don't have convergence requirement.

EIGRP Stub is used to avoid spoke site being transit network for the other spoke sites. Also EIGRP Stub node doesn't receive EIGRP query, which is good optimization mechanism for the EIGRP network.

We know that there is no spoke to spoke communication and also spoke routers should be prevented to be used as the transit node for the subnets behind other spoke routers or the Hub router in case Dual Hub design.

EIGRP Stub always should be used at the Edge of the network such as Spoke routers in the Hub and Spoke topology.

Correct answer of this question is EIGRP Stub feature, which is Option C.

Question 18 : Do you think that running EIGRP over the GRE tunnels on this network improves the resiliency ?

A- YES

B- NO

Answer 18 : If you remember the GRE tunnel physical design, there is only one GRE tunnel per store. Which mean even there is EIGRP running over the tunnel, there is no alternate path to converge.

With this question, exam is looking whether you can follow the changes, are you answering the question based on the business

and technical requirements which are given in the scenario or just based on the design best practices.

That's why Answer is No, which is Option B.

Question 19: Could you use BGP instead of EIGRP on this network ?

A – YES
B- NO

Answer 19 – Yes it could be used. The detail answer will be provided in Answer 20.

Question 20: What would be the two reasons to choose BGP over EIGRP? (Choose two)

A- BGP will be easier to configure on the Hub router

B – BGP can converge faster

C- BGP provides better filtering and policy capability

D- With BGP tunnel bandwidth requirement can be reduced

E- BGP scales to a much higher neighbor count

Answer 20: BGP will not be easier than EIGRP from the configuration point of view. Actually it is going to be even harder since the BGP requires neighbor statement configuration on each router.

That's why Option A is not correct.

BGP doesn't provide faster converge than EIGRP. With BGP PIC dataplane convergence optimization, BGP can provide Fast Reroute but all the routing protocols with some enhancement can provide fast reroute. Since by default, control plane convergence of BGP is slower than EIGRP, Option B is incorrect.

BGP is a policy protocol first, routing protocol second.

BGP provides best filtering and policy capability among all the routing protocols. One of the correct answers is Option C.

BGP doesn't consume more or less bandwidth than the other routing protocols that's why Option D is incorrect.

BGP is known as the most scalable protocol. That is definitely true since it is invented to support entire Internet.

Correct answer should be Option C and Option E.

Question 21: MILKATURKA wants to implement VTP in the Headquarter, would you recommend it?

A- YES
B- NO

Answer 21 : Answer is No. VTP provides simplified operation in the large scale LAN environment by centralizing the Vlan configuration and distribution.

There are three reasons to not to enable VTP in this network.

First reason, there is really small number of VLan and scenario don't mention whether many new Vlan will be added. Also number of switch is important for the Vlan configuration. Small number of Vlan (21total as it is given in the background information) easily can be managed manually.

Second reason, this is brownfield environment, which mean, VLAN configuration is working already and again there is no mention for the rapid VLAN number grow.

Third reason is, mistake in the VTP configuration can create network wide failure.

If the older revision number switch is added to the VTP domain as a VTP server, all the other switches accept and override the new VTP configuration. This creates network wide failure. That's why the best practice for the VTP; don't enable it since the impact of misconfiguration always greater than its benefit.

Question 22 : MILKATURKA wants to identify which applications are consuming the most bandwidth and which IP address is creating the most amount of traffic for their front stores. Which below options provide this information? (Choose all that apply)

A- SNMP
B- Syslog
C- Netflow
D- IPFIX

Answer 22 : They are basically looking flow information for their 480 front stores. SNMP and syslog don't provide the detail flow information such as which IP address creating the most amount of traffic and which application is heavily used and so on.

Netflow and IPFIX are used for this purpose.

Question 23: Which below technology provides standard base flow information?

A- IPFIX

B- Netflow
C- Radius
D- TACACS
E- Sflow

Answer 23: TACACS and Radius don't provide flow information. They are not used for that purpose.
Sflow and Netflow vendor specific protocols, which provide flow information. They could be chosen but the question is asking standard base protocol, which is RFC 5101.

Question 24: MILKATURKA realized that they don't use their one of the uplink for the Internet on the Internet Gateway Router after they enabled the IPFIX. They want to use both link as active-active. Which below information do you need to recommend them a solution? (Choose all that apply)

A- IGP configuration
B- Internet Gateway configuration
C- Ingress and Egress bandwidth utilization
D- BGP Configuration

Answer 24: IGP configuration is not important for the Internet usage for this question it should be obvious.

Ingress and Egress bandwidth utilization information we don't need since the question already provided this information actually. In the question it is stated that one of the uplink is not used at all. It can be 10% or 90% , we still need to start use the other link or links.

We don't know how many links they have , whether they have Static route or BGP on the router for the Internet as well.

Since we don't know whether they use BGP for the internet Option D is incorrect as well. They might be using Static route.

We only need Internet Gateway configuration, so we can understand how many links they have, whether they have static route or BGP, If it is BGP, what is the BGP configuration, how many service provider and BGP policy for those and so on.

Mail 2 is Available

We sent our Internet Gateway Router configuration at the attachment. As you can see we are using BGP on the router, we have only one Internet service provider. We have two circuits and over each circuit we have separate BGP sessions and advertise our Service Provider assigned IP address block. And there is no specific BGP policy currently other than prefix advertisement.

Please help us to use the second link as well since we don't want it to be idle.

Question 25: Which below BGP parameters can help MILKATURKA to start utilizing their second link as well ?

A- BGP MED
B- As-Path Prepend
C- Community
D- Weight
E- Origin

Answer 25 : Since they have two BGP sessions over two links and one of the link is not carrying any traffic, those sessions are terminated on the same router at the Service Provider site.

If it would be at the different routers, because of Service Providers first choose Hot Potato for BGP, second router would be used by some BGP routers in the service provider network that's why second link of the customer would be used.

When both links on the same router at the service provider site, all the other BGP routers in the service provider has only have one egress router which is connected to the MILKATURKA.

The service provider router, which is connected to the MILKATURKA selects only one link based on the BGP best path selection algorithm and uses only one best path.

None of the above attributes are needed since there is better option for the particular problem.

Either static route is written for the loopback addresses of the service provider towards both circuits and BGP session is setup from the loopback interfaces or two links are terminated on the different routers on the Service provider site and BGP attributes are used to solve the utilization problem.

When loopback address is used, MILKATURKA would have only one BGP sessions through two physical link and two static routes, both for the same loopback interface of the remote SP BGP router towards two interface addresses.

Question 26 : Customer asked from their service provider the second circuit to be terminated on the different BGP router. Which below options can provide download traffic of the MILKATURKA to be carried over both links? (Choose all that apply)

A- BGP MED
B- AS Path Prepend
C- BGP Communities
D- Weight
E- Local Preference
F- Nothing is required, it would work

Answer 26 : Since the requirement is to carry upload traffic, inbound traffic optimization BGP attributes are needed.

BGP MED , As Path prepend and the communities are used to influence inbound traffic utilization with the BGP.

Bgp MED is used when the customer is connected to the one Service provider only. In this network, customer is using only one service provider that's why BGP MED can be used to influence inbound traffic.

BGP weight is Cisco proprietary BGP attribute which is used to influence outbound traffic but it is effective only on the local router. We are looking inbound optimization that's why Option D is not correct. Local preference is domain wide attribute but it is used for outbound BGP traffic optimization as well.

Question 27 : Is this enough to satisfy MILKATURKA link usage requirement ?

A- Yes
B- No

Answer 27 : No it is not. Since MILKATURKA wants to use second link as well, it is not only inbound but also outbound traffic needs to be used. Outbound traffic is handled by the Local preference attribute in general but in this network it could be the weight attribute as well since customer has only one BGP router.

If next question would asked which one is best, Local Preference or Weight then the answer would be Local Preference since Weight is Cisco proprietary as it is stated earlier in the Answer 26, so solution would be locked in to one vendor also weight is local to the router. Which mean , when MILKATURKA wants to add second BGP router and carry the second link over that router for the

resiliency purpose, weight would be useless. That's why starting with Local preference to influence outbound traffic (download) would be the best BGP policy.

Question 28 : MILKATURKA wants to hardened the BGP router. Which features below provide DDOS protection on their BGP router ? (Choose all that apply)

A- SSH
B- uRPF strict mode
C- CoPP
D- uRPF loose mode
E- NTP
F- GTSM

Answer 28 : SSH is used to access the networking devices securely. It is chosen over Telnet since SSH provides encryption but telnet doesn't. But SSH doesn't provide DDOS protection.

uRPF, Unicast Reverse Path Forwarding has two flavors; uRPF strict mode and uRPF loose mode. Both are used to provide DDOS protection.

uRPF when is used in conjunction with BGP allows traffic to dropped if comes from the spoofed source address. It can protect the network against destination based attacks as well. Strict mode requires IP address to interface matching, loose mode doesn't require. So strict mode allows only symmetrical traffic flow but loose mode allows asymmetrical flows as well.

CoPP, Control plane policy protection, protects the router control plane from the DDOS attacks. CoPP is definitely one of the correct answers.

NTP, Network Time Protocol is not related with the DDOS attacks.

GTSM; Generalized TTL Security Mechanism initial TTL value for an eBGP packet is set to 255 rather than 1, and a minimum TTL-value is enforced on all BGP packets that are associated with that eBGP session. Because the IP header TTL value is decremented by each router hop along its path to its final destination, the diameter from which an attacker could possibly source packets is restricted to those routers that are directly connected. GTSM is one of the main tools to provide DDOS protection on the Internet Gateways.

Correct answers are Options B, C, D and F.

Questions 29 : One of the MILKATURKA network engineer suggested to use BGP MD5 Authentication as well to protect the Internet Gateway from the DDOS attacks since as per him, when it is used with GTSM, it provides additional layer of DDOS protection. Would you agree with this engineer?

A- Yes
B- No

Answer 29 : MD5 Authentication is used against to Route Manipulation attack.

By enabling the MD5-based neighbor authentication mechanism, administrators can ensure that only authorized peers can establish this BGP neighbor relationship, and that the routing information exchanged between these two devices has not been modified. GTSM as it is explained in the Answer 28 is used for DDOS protection.

MD5 Authentication cannot add any benefit to GTSM for DDOS protection and actually its exacerbate GTSM's effect because MD5 Authentication causes the router CPU to consume more resources while it attempts to compute MD5 hashes on large numbers of attack packets.

That’s why answer is Option B for this question.