PassQueen
a.k.a dumpsqueen.com

Nuage Networks Virtualized Network Services (VNS) Fundamentals

Nokia 4A0-N02

Version Demo

Total Demo Questions: 6

Total Premium Questions: 60

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

What type of NAT is used so that any external host can send to iAddr: iPort by sending traffic to eAddr: ePort? (i=internal, e=external)

A. Full-cone NAT

B. Address-restricted NAT

C. Port-restricted NAT

D. Symmetric NAT

ANSWER: A

Explanation:

Full-cone NAT is correct because it creates a persistent public mapping from the internal endpoint, iAddr:iPort, to a specific external endpoint, eAddr:ePort. Once that mapping exists, the NAT device forwards traffic sent to eAddr:ePort to the mapped internal iAddr:iPort regardless of the source address or source port of the external sender. In other words, any Internet host can initiate traffic toward the mapped public address and port, provided the mapping remains active. This unrestricted inbound reachability is the defining behavior of full-cone NAT and is why it is also commonly called one-to-one NAT in NAT-behavior classifications. The terminology in the question—internal address/port and external address/port—matches the endpoint notation used in standard NAT traversal documentation. RFC 3489 defines a full-cone NAT as one where all packets received at the mapped external address and port are forwarded to the internal host, independent of the external packet's source endpoint. See RFC 3489, Section 5. For broader NAT behavioral terminology and endpoint-mapping context, consult RFC 4787: Network Address Translation Behavioral Requirements.

QUESTION NO: 2

Which component is responsible for maintaining control-plane state and distributing forwarding information to the VRSs and NSGs?

A. VSD (Virtualized Services Directory)

B. VSC (Virtualized Services Controller)

C. VRS (Virtual Routing and Switching)

D. VSAP (Virtualized Services Assurance Platform)

ANSWER: B

Explanation:

VSC (Virtualized Services Controller) is correct. The VSC is the distributed control-plane component in the Nuage VNS architecture. It receives the service intent and policy information derived from the VSD and communicates the required forwarding, reachability, tunnel, and policy state to the data-plane elements, including VRSs and NSGs.

The VSD is the management and policy-definition component, whereas VRSs and NSGs enforce the resulting forwarding behavior in the data plane. Additional Nuage architecture documentation is available through the Nokia Nuage documentation portal.

QUESTION NO: 3

Which of the following statements is correct regarding an L2 domain in the Nuage VNS service model?

A. It provides a Layer 2 broadcast domain for attached endpoints.

B. It is the VSD abstraction that corresponds to a VRF.

C. It can contain multiple Layer 3 domains.

D. It is used only to configure NSG WAN interfaces.

ANSWER: A

Explanation:

It provides a Layer 2 broadcast domain for attached endpoints. is correct. An L2 domain represents a virtual Ethernet segment to which vPorts can be connected. Endpoints attached to the same L2 domain can exchange Layer 2 traffic according to the configured forwarding and security policies.

Unlike a Layer 3 domain, an L2 domain is not the routed VRF-like context used to organize zones and IP subnets. Routing between distinct IP networks requires an appropriate Layer 3 service design. The VNS service model and associated virtual networking concepts are described in the Nokia Nuage documentation portal.

QUESTION NO: 4

Which of the following is FALSE regarding VNS bootstrapping?

A. The bootstrapping configuration templates on VSD ensures NSG configuration conformance.

B. NSG is ready for dispatch without prior configuration.

C. It solves the problem of site CPE activation without having to send a skilled technician on site.

D. NSG exchanges the plain text proprietary bootstrap protocol with VSD.

ANSWER: D

Explanation:

“NSG exchanges the plain text proprietary bootstrap protocol with VSD.” is the false statement. VNS bootstrapping is designed to allow an NSG to be shipped to a site with no site-specific preconfiguration and then securely obtain its operating configuration from the Virtualized Services Directory. This process must protect both the identity of the gateway and the configuration data that defines tenant connectivity and service behavior. The NSG therefore establishes an authenticated, encrypted management connection to the VSD rather than exchanging bootstrap information through a plain-text protocol. Certificate-based identity and TLS-protected HTTPS communication are fundamental to preventing interception, modification, or unauthorized retrieval of bootstrap and configuration information while the device is connected through an untrusted access network. After secure authentication, the VSD can apply the appropriate bootstrap configuration and templates, enabling centralized and consistent deployment of the NSG. Nokia’s Nuage documentation portal provides product documentation for VSD and NSG deployment and security procedures at Nokia Nuage documentation. Nokia also describes its service-routing and cloud networking portfolio, including secure automated service delivery, at Nokia IP Routing.

QUESTION NO: 5

Which of the following is correct about the NAT/PAT function on the NSG?

A. Only one mode (either NAT or PAT) is supported, depending on administrative configuration.

B. NAP/PAT is used to offload the Internet traffic.

C. By default, NAT/PAT is enabled.

D. NAT/PAT is enabled at the NSG level and applied to all network ports.

ANSWER: B

Explanation:

“NAP/PAT is used to offload the Internet traffic.” is correct, with “NAP” evidently intended to mean NAT. In Nuage VNS deployments, an NSG at a branch location can provide local Internet breakout. NAT/PAT translates private enterprise addresses and, for PAT, multiplexes multiple internal flows over one or more public-facing addresses and transport ports. This lets Internet-destined traffic leave through the branch’s local Internet connection rather than being carried across the WAN overlay to a centralized data center or security gateway. The function is therefore commonly described as Internet offload or local Internet breakout. It helps reduce unnecessary WAN backhaul, lowers latency for suitable Internet and SaaS traffic, and preserves the use of private addressing within the enterprise site. NAT/PAT policy is applied in the context of the relevant NSG/enterprise network configuration so that the selected traffic is translated as it exits toward the Internet. Nokia’s NSG is the branch gateway component of the Nuage VNS architecture and supports such branch connectivity services. See Nokia’s Nuage Networks product information and Nokia technical documentation portal for platform and deployment documentation.

QUESTION NO: 6

Which of the following statements about uplink ingress policing is FALSE?

A. It can be applied to the overlay.

B. It can be applied to the underlay.

C. VSD raises an alarm when the policing threshold is crossed.

D. The policer can be configured by enterprise admin.

ANSWER: B

Explanation:

“It can be applied to the underlay.” is the false statement. Uplink ingress policing in Nuage VNS is an overlay-service policy function. It controls the rate of traffic entering an uplink in the context of the virtualized network service and its associated policy domain, rather than policing the physical IP fabric that provides transport between infrastructure components. The underlay must remain available to carry the encapsulated overlay traffic and related network transport functions; it is not the target of this VSD-configured uplink ingress policing feature. In contrast, applying the policy to overlay traffic enables the service operator to enforce an agreed traffic rate at the service boundary while retaining centralized visibility and control through the Virtualized Services Directory. VSD can generate alarms when configured policing thresholds are crossed, allowing the enterprise administrator to monitor service consumption and respond to sustained threshold events. This distinction between centrally managed overlay service policy and the independent transport underlay is fundamental to the Nuage VNS architecture. See Nokia’s Nuage Virtualized Services Platform overview and the Nokia Network Automation documentation for VSD-managed virtual network policy concepts.