AZ-700 · CHEAT SHEET · CERTIFYDECK

Microsoft Certified: Azure Network Engineer Associate

Nivel: Intermediate (Associate) Duración: 100 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Design and implement core networking infrastructure

25–30%

Design and implement IP addressing for Azure resources

- Cada red virtual que vayas a conectar con otras redes o con la red local necesita un espacio de direcciones que no se solape, y Azure reserva cinco direcciones en cada subred (las cuatro primeras y la última). Puedes ampliar o reducir un rango mientras siga conteniendo sus subredes; en una red emparejada, cada cambio de rango exige sincronizar el emparejamiento.
- Una red virtual pertenece a una sola región y suscripción, y los recursos que se conectan a ella deben estar en la misma región; para otra región se crea otra red y se empareja. Al crearla defines uno o varios rangos CIDR sin solapes (privados RFC 1918, RFC 6598 o públicos propios), nunca los de vínculo local, multidifusión, bucle invertido o 168.63.129.16.
- Varios servicios exigen subredes con nombre reservado y sin otros recursos: GatewaySubnet para las puertas de enlace, AzureFirewallSubnet (y AzureFirewallManagementSubnet si se habilita la NIC de administración) para Azure Firewall y AzureBastionSubnet para Azure Bastion. Application Gateway usa una subred dedicada con el nombre que elijas, mientras que los puntos de conexión privados y de servicio se configuran en subredes normales.
- La delegación de subred concede a un servicio PaaS permiso para crear sus recursos en una subred concreta, por ejemplo Microsoft.Sql/managedInstances o Microsoft.Web/serverFarms. El propietario sigue pudiendo aplicar NSG y rutas, pero una subred delegada no admite puntos de conexión privados y la delegación no se puede quitar mientras haya recursos del servicio desplegados.
- Algunos servicios exigen una subred dedicada en la que solo puede haber recursos suyos (Route Server, SQL Managed Instance, Application Gateway, las puertas de enlace en GatewaySubnet), mientras que máquinas virtuales, aplicaciones virtuales de red y puntos de conexión privados pueden compartir subred. En una subred compartida, los NSG solo afectan a los puntos de conexión privados si se habilita su directiva de red.

Design and implement name resolution

- Dentro de una red virtual puedes usar la resolución proporcionada por Azure (sin configuración, limitada a esa red), zonas de Azure Private DNS (la opción preferida), Azure DNS Private Resolver o tus propios servidores DNS que reenvían a 168.63.129.16. El DNS inverso administrado por Azure se limita a cada red; para abarcar varias se usa una zona privada in-addr.arpa con registros PTR manuales.
- La configuración de servidores DNS de una red virtual puede ser Predeterminado (proporcionado por Azure) o una lista de servidores personalizados, que se usan en orden y no en round-robin. La configuración DNS de una NIC invalida la de la red, y tras cualquier cambio las VM existentes deben renovar la concesión DHCP o reiniciarse para aplicarlo.
- Una zona pública de Azure DNS aloja los registros de un dominio y se publica delegando en sus cuatro servidores de nombres desde el registrador; los subdominios se delegan con un conjunto de registros NS en la zona primaria. En el vértice no puede haber CNAME, por lo que se usan registros de alias que además siguen el ciclo de vida de IP públicas o perfiles de Traffic Manager y evitan registros huérfanos.
- Una zona de Azure Private DNS es un recurso global que resuelve nombres solo para las redes virtuales vinculadas, en cualquier región y sin necesidad de emparejamiento. Admite horizonte dividido con una zona pública del mismo nombre; el registro automático crea registros A solo para las VM y cada red puede tener una única zona de registro, así que otros recursos se registran a mano.
- Las zonas públicas se crean con az network dns zone create y las privadas con az network private-dns zone create; los registros usan nombres relativos y se agrupan en conjuntos por nombre y tipo, con un TTL por conjunto. Una zona pública se publica actualizando en el registrador los registros NS con sus servidores de nombres, y una zona privada se resuelve solo desde las redes virtuales vinculadas.

Design and implement VNet connectivity and routing

- El encadenamiento de servicios dirige el tráfico de un spoke a una NVA o a una puerta de enlace de VPN de una red emparejada mediante rutas definidas por el usuario. El tránsito de puerta de enlace se habilita en el hub y el uso de puertas de enlace remotas en el spoke, que no puede tener su propia puerta de enlace. No se puede enrutar entre redes virtuales con una ruta cuyo próximo salto sea una puerta de enlace de ExpressRoute.
- El emparejamiento conecta redes virtuales de la misma región o de regiones distintas por la red troncal de Microsoft. Requiere espacios de direcciones sin solapamiento y un emparejamiento en cada red: el primero queda en Initiated hasta que se crea el recíproco. No es transitivo, no resuelve nombres con el DNS predeterminado de Azure y hay que eliminarlo antes de mover la red virtual.
- Azure Virtual Network Manager agrupa redes virtuales en grupos de red, con pertenencia estática o dinámica mediante Azure Policy, y les aplica configuraciones de conectividad en malla o en estrella. La conectividad directa crea un grupo conectado regional que la malla global extiende entre regiones. Nada surte efecto hasta implementarlo por región, y cada implementación fija el estado objetivo de esa región.
- Las rutas definidas por el usuario se crean en una tabla de rutas e invalidan las rutas del sistema. Admiten los próximos saltos VirtualAppliance, VirtualNetworkGateway (solo con puerta de enlace de VPN), VnetLocal, Internet y None, y pueden usar etiquetas de servicio como prefijo. Una NVA usada como próximo salto necesita el reenvío IP habilitado en su NIC y debe estar en otra subred para evitar bucles.
- Una tabla de rutas se asocia a subredes, nunca a la red virtual, y cada subred admite como máximo una. Solo puede asociarse a subredes de la misma ubicación y suscripción que la tabla, y no se puede eliminar mientras siga asociada. No se debe asociar a GatewaySubnet una tabla con 0.0.0.0/0 si hay una puerta de enlace de VPN; al desasociarla, la subred vuelve a las rutas predeterminadas.

Monitor networks

- Network Watcher se habilita por región, en NetworkWatcherRG. Los registros de flujo de red virtual se guardan en una cuenta de almacenamiento estándar de la misma región y pueden configurarse en NIC, subred o red virtual, con prioridad en ese orden; el análisis de tráfico necesita un área de trabajo de Log Analytics. Connection monitor y la captura de paquetes necesitan agentes y la captura en almacenamiento requiere acceso con clave.
- Network Watcher reúne herramientas de diagnóstico: la comprobación del flujo de IP indica qué regla permite o deniega un flujo TCP o UDP, el diagnóstico de NSG cubre también ICMP y etiquetas de servicio, y las reglas de seguridad efectivas agregan NIC y subred. La solución de problemas de conexión prueba en un momento dado, mientras que Connection monitor supervisa de forma continua la latencia y la pérdida.
- Azure Monitor Network Insights, antes llamado Azure Monitor for Networks, muestra sin configuración previa la topología, el estado, las métricas y las alertas de todos los recursos de red en varias suscripciones. Su vista de conectividad depende de pruebas de Connection monitor, la de tráfico de los registros de flujo y del análisis de tráfico, y el kit de diagnóstico abre las herramientas de Network Watcher.
- DDoS Network Protection se activa vinculando redes virtuales a un plan de protección, que sirve para varias suscripciones del mismo inquilino e incluye respuesta rápida y protección de costes; DDoS IP Protection se habilita en cada IP pública Standard sin plan. Para supervisar, usa la métrica Under DDoS attack or not en alertas y las categorías DDoSProtectionNotifications y DDoSMitigationFlowLogs en Log Analytics.
- La puntuación de seguridad agrupa las recomendaciones de Microsoft cloud security benchmark en controles como Secure management ports o Restrict unauthorized network access, un control suma todos sus puntos cuando todos los recursos cumplen todas sus recomendaciones, y las recomendaciones en versión preliminar no cuentan. Puedes corregir con Fix, evitar regresiones con Enforce o Deny y consultar los controles con Azure Resource Graph.

2. Design, implement, and manage connectivity services

20–25%

Design, implement, and manage a site-to-site VPN connection

- Una puerta de enlace VPN tiene dos instancias, activa-en espera por defecto; el modo activo-activo da una IP pública por instancia y exige que el dispositivo local establezca un túnel con cada una. Para la máxima disponibilidad se combina con dos dispositivos locales, una puerta de enlace de red local y una conexión por dispositivo, y BGP. La redundancia de zona requiere una SKU AZ e IP públicas Standard con redundancia de zona.
- Para gateways VPN nuevos se usan las SKU AZ (VpnGw1AZ a VpnGw5AZ), que admiten BGP, activo-activo, directivas IPsec/IKE personalizadas y redundancia de zona; las SKU sin AZ se migran y no sirven para crear gateways. NAT requiere VpnGw2AZ o superior. Basic es solo para desarrollo: sin BGP, RADIUS, IPv6, activo-activo ni redundancia de zona.
- Una conexión de sitio a sitio une una puerta de enlace VPN basada en rutas con una puerta de enlace de red local mediante una clave compartida que debe coincidir con la del dispositivo local. En modo activo-activo el dispositivo debe tener un túnel hacia cada IP pública, y ambos túneles forman una sola conexión. Connection Mode define quién inicia IKE y el estado se comprueba con az network vpn-connection show.
- Las VPN basadas en directivas cifran según combinaciones de prefijos y solo existen en la SKU Basic con IKEv1; las basadas en rutas usan selectores de cualquiera a cualquiera y son las necesarias para punto a sitio, BGP y activo-activo. El tipo no se puede convertir. Para dispositivos locales basados en directivas, usa una puerta de enlace basada en rutas con directiva IPsec/IKE personalizada y UsePolicyBasedTrafficSelectors.
- La puerta de enlace de red local representa el sitio y su dispositivo VPN: guarda la IP pública o un FQDN del dispositivo, los prefijos locales que Azure enruta hacia él y, con BGP, la IP del par BGP y el ASN local. Al cambiar prefijos con Set-AzLocalNetworkGateway se sobrescriben los anteriores, y modificarla con una conexión activa puede romper el túnel.

Design, implement, and manage a point-to-site VPN connection

- Para punto a sitio se necesita una puerta de enlace basada en rutas; en implementaciones nuevas se usa una SKU AZ, porque Basic admite IKEv2 con certificados pero no OpenVPN, RADIUS, IPv6 ni activo-activo, y por tanto tampoco Microsoft Entra ID. El número de conexiones P2S depende de la SKU, y una puerta de enlace activa-activa con P2S necesita una tercera IP pública.
- Punto a sitio admite OpenVPN (TLS sobre TCP 443, multiplataforma y único compatible con Microsoft Entra ID), IKEv2 (IPsec sobre UDP 500 y 4500) y SSTP (TLS solo para Windows, en retirada). SSTP e IKEv2 pueden convivir, pero SSTP y OpenVPN no. Tras cambiar el tipo de túnel o la autenticación hay que generar y distribuir un nuevo paquete de configuración del cliente VPN.
- Una puerta de enlace P2S admite tres tipos de autenticación: certificado de Azure, Microsoft Entra ID y RADIUS con Active Directory, y puedes combinarlos. Microsoft Entra ID solo funciona con OpenVPN y el Azure VPN Client, y aporta acceso condicional y MFA; RADIUS reenvía la autenticación a tu servidor y permite usar tu PKI sin cargar certificados raíz en Azure.
- Con RADIUS, la puerta de enlace VPN basada en rutas reenvía la autenticación a tu servidor (por ejemplo NPS), que se registra como cliente RADIUS con la GatewaySubnet y el mismo secreto compartido. Puedes indicar dos servidores para alta disponibilidad. Si el servidor está en el entorno local, hace falta una VPN de sitio a sitio; ExpressRoute no sirve para llegar a él, y la SKU Basic no admite RADIUS.
- La autenticación de Microsoft Entra ID usa OpenVPN y el Azure VPN Client, y se configura en la puerta de enlace con los valores de Tenant, Audience e Issuer. Con la aplicación registrada por Microsoft no hay que registrar nada en el inquilino. Cada puerta de enlace admite una sola Audience; para limitar el acceso por grupos se usa una aplicación de auditoría personalizada por puerta de enlace.

Design, implement, and manage Azure ExpressRoute

- ExpressRoute ofrece cuatro modelos: colocalización en CloudExchange, Ethernet de punto a punto, cualquiera a cualquiera (IPVPN) y ExpressRoute Direct. Con proveedores de capa 2 configuras tú el enrutamiento BGP; los proveedores IPVPN suelen gestionar la capa 3. Direct da puertos dedicados y aislados físicamente, con MACsec opcional entre tus enrutadores y los de Microsoft.
- Los circuitos tienen tres SKU: Local (una o dos regiones cercanas a la ubicación de emparejamiento, transferencia incluida y sin Global Reach), Standard (todas las regiones de su zona geopolítica) y Premium (conectividad global y Microsoft 365). La familia de facturación es MeteredData o UnlimitedData; puedes subir de Standard a Premium, pero no pasar de UnlimitedData a MeteredData.
- Cada circuito tiene dos conexiones activas; mantenlas en equipos locales distintos y usa puertas de enlace con redundancia de zona y BFD. Para recuperación ante desastres, usa circuitos en distintas ubicaciones de emparejamiento y prefiere uno con rutas más específicas, peso de conexión o anteposición de AS path, cuidando la simetría. Fuera de la región geopolítica hace falta Premium; una VPN de sitio a sitio sirve de respaldo activo-pasivo.
- Global Reach une los emparejamientos privados de dos circuitos para conectar sitios locales por la red de Microsoft, con una subred /29 propia y Premium solo entre regiones geopolíticas. FastPath envía el tráfico directamente a las VM omitiendo la puerta de enlace y exige SKU como ErGw3Az; con Direct admite además emparejamiento en la misma región y UDR. Direct ofrece puertos dedicados con MACsec.
- El emparejamiento privado de Azure extiende tu red a las redes virtuales y a sus puntos de conexión privados con direcciones privadas. El emparejamiento de Microsoft llega a Microsoft 365 y a servicios públicos de Azure con IP públicas registradas, normalmente con NAT, y algunos servicios como Front Door no se admiten. Puedes habilitar ambos en el mismo circuito, con sesiones BGP separadas.

Design and implement an Azure Virtual WAN architecture

- Una WAN virtual Basic solo contiene centros virtuales Basic, limitados a VPN de sitio a sitio, sin router de tránsito ni ajuste de unidades de escalado. Standard añade ExpressRoute, User VPN de punto a sitio, tránsito entre redes virtuales y entre centros virtuales, Azure Firewall y NVA en el centro virtual. Se puede pasar de Basic a Standard, pero nunca volver a Basic.
- Virtual WAN implementa una red de tránsito global en estrella: los centros virtuales de cada región se conectan en malla completa y ofrecen tránsito de cualquier punto a cualquier punto entre sucursales, usuarios remotos y redes virtuales, incluso de otra región. Cada red virtual se conecta a un solo centro. Branch-to-Branch puede deshabilitarse, y el tráfico se inspecciona con Azure Firewall o NVA mediante la intención de enrutamiento.
- Un centro virtual es una red virtual administrada por Microsoft con un router que gestiona el tránsito; puede crearse vacío y recibir las puertas de enlace después. Su espacio de direcciones no se puede cambiar tras crearlo y no debe solaparse con otros centros, el entorno local ni las redes conectadas; dimensiónalo pensando en Azure Firewall o NVA. Si el enrutamiento queda en Failed, usa Reset Router.
- Las unidades de escalado fijan el rendimiento agregado de cada puerta de enlace del centro virtual y se configuran por separado para sitio a sitio, User VPN y ExpressRoute; la de sitio a sitio se dimensiona con el total de las sucursales. No hay que confundirlas con las unidades de infraestructura de enrutamiento del router, que se suben para más máquinas virtuales. Cambiarlas puede causar reconexiones breves.
- Las puertas de enlace de sitio a sitio, User VPN y ExpressRoute se crean al crear el centro virtual o después, editándolo, y sustituyen a las de las redes virtuales, que deben quitarse antes de conectarlas al centro. Los circuitos Local, Standard y Premium pueden conectarse. Propagate Default Route solo reenvía una ruta predeterminada que el centro ya haya aprendido, por ejemplo de un firewall.

3. Design and implement application delivery services

15–20%

Design and implement Azure Load Balancer and Azure Traffic Manager

- Azure Load Balancer trabaja en la capa 4 con TCP y UDP. Sus componentes son la IP de front-end (pública o privada), el grupo de back-end, los sondeos de estado TCP, HTTP o HTTPS, las reglas de equilibrio de carga (solo entrantes, con afinidad por IP de origen opcional), los puertos HA en equilibradores internos, las reglas NAT de entrada para reenviar puertos y las reglas de salida para SNAT.
- Usa Azure Load Balancer para tráfico TCP o UDP de capa 4 entre máquinas virtuales o conjuntos de escalado: público para tráfico de internet e interno para tráfico privado, también desde el entorno local. También sirve para dar salida a internet con SNAT, reenviar puertos y escalar NVA con puertos HA. Para capa 7 se usan Application Gateway o Front Door, y Traffic Manager funciona solo mediante DNS.
- Las SKU vigentes son Standard y Gateway; Basic está retirada. Standard admite front-end públicos o internos con redundancia de zona, sondeos HTTPS, puertos HA en internos y reglas de salida, y tiene un nivel Global, solo público, que pone una IP anycast delante de equilibradores regionales (no se actualiza desde uno regional). Gateway inserta NVA de forma transparente y se encadena a un front-end público.
- El tipo de front-end decide el tipo de equilibrador: una IP pública crea un equilibrador público y una IP privada crea uno interno, que solo atiende a la red virtual y a redes conectadas, como la red local por VPN o ExpressRoute, y nunca acepta tráfico de internet. Los equilibradores Standard están cerrados por defecto y necesitan un NSG que permita el tráfico. Una VM de back-end no puede llegar al front-end de su propio equilibrador interno.
- Un equilibrador regional reparte tráfico entre VM de una red virtual, el nivel Global de Load Balancer añade una IP pública anycast estática delante de equilibradores regionales públicos de varias regiones, conserva la IP del cliente y saca de la rotación la región que falla. Se crea nuevo (no se actualiza uno regional), no admite reglas de salida ni front-end interno, y su puerto de back-end debe coincidir con el front-end regional.

Design and implement Azure Application Gateway

- Application Gateway v2 es un equilibrador de capa 7 con terminación TLS y TLS de extremo a extremo, escalado automático, redundancia de zona, IP virtual estática, enrutamiento por ruta URL y por host, redirección, reescritura de encabezados y URL, afinidad de sesión por cookies, purga de conexiones, páginas de error personalizadas, WebSocket y HTTP/2, y WAF en el nivel WAF_v2. Cada requisito se asigna a una de estas capacidades.
- Application Gateway encaja cuando una aplicación web regional necesita decisiones de capa 7 dentro de la red virtual: enrutamiento por ruta o host, terminación TLS, WAF o afinidad por cookies, con front-end público o privado para aplicaciones internas. También sirve de entrada para AKS con AGIC y admite back-end locales con conectividad IP. Para UDP se usa Load Balancer, y para distribución global, Front Door o Traffic Manager.
- Application Gateway v2 escala en modo automático o manual. El automático amplía y reduce instancias según el tráfico, con un mínimo obligatorio que mantiene capacidad base mientras se aprovisionan nuevas instancias y un máximo opcional. El manual fija un número de instancias que no cambia y puede perder tráfico si se supera, así que se dimensiona según el pico con margen. En ambos casos la subred dedicada debe tener una IP por instancia.
- Un grupo de back-end de Application Gateway puede contener NIC, conjuntos de escalado, IP públicas o internas, FQDN y servicios multiinquilino como App Service, dentro o fuera de la red virtual si hay conectividad IP (emparejamiento, VPN o ExpressRoute). Los FQDN se resuelven con el DNS de la red virtual, y tras cambiar sus servidores hay que detener e iniciar la puerta de enlace. App Service sin dominio propio exige invalidar el host.
- Application Gateway sondea cada combinación de servidor y configuración de back-end desde todas sus instancias y deja de enviar tráfico a los servidores incorrectos. El sondeo predeterminado usa el protocolo y puerto de la configuración de back-end, el host 127.0.0.1 y acepta códigos 200-399. Un sondeo personalizado permite fijar host, ruta, puerto, intervalo, umbral y criterios de coincidencia de código o cuerpo; MinServers exige cautela.

Design and implement Azure Front Door

- Azure Front Door es una CDN y equilibrador global de capa 7 solo para HTTP y HTTPS. Ofrece cuatro métodos de enrutamiento hacia los orígenes (latencia, prioridad, ponderado y afinidad de sesión), sondeos de estado por grupo de orígenes, almacenamiento en caché, compresión, motor de reglas, WAF y certificados administrados. Admite orígenes en Azure, en local o en otras nubes como Custom host.
- Front Door es la opción para aplicaciones web HTTP(S) públicas desplegadas en varias regiones que necesitan caché en el perímetro, aceleración, conmutación rápida y WAF. No sirve para tráfico no HTTP (TCP o UDP), que va a Load Balancer o Traffic Manager, ni para aplicaciones solo internas, donde encaja Application Gateway; su Private Link protege solo el tramo de Front Door al origen.
- Front Door Standard incluye entrega estática y dinámica, caché, compresión, motor de reglas con regex y variables de servidor, dominios personalizados y WAF con reglas personalizadas y filtrado geográfico. Premium añade el conjunto de reglas administrado, protección contra bots, Private Link hacia el origen y mTLS de clientes. Standard se actualiza a Premium sin reconstruir, pero no hay bajada directa; los clásicos no admiten perfiles nuevos.
- Un perfil de Front Door contiene puntos de conexión con un dominio azurefd.net generado, rutas que asocian dominios, protocolos y patrones de ruta a un grupo de orígenes, y orígenes con prioridad, peso y encabezado de host. La coincidencia elige la ruta más específica: primero ruta exacta y luego comodín; sin coincidencia devuelve 404. Los grupos de orígenes definen sondeos de estado y equilibrio de carga.
- Front Door termina TLS en el PoP con un certificado administrado (recomendado, con rotación automática si el CNAME apunta directamente al punto de conexión) o con uno propio guardado en Key Vault de la misma suscripción. Para TLS de extremo a extremo se reenvía con HTTPS y el origen debe presentar un certificado de una entidad de confianza cuyo nombre de firmante coincida con su nombre de host.

4. Design and implement private access to Azure services

10–15%

Design and implement Azure Private Link service and Azure private endpoints

- Un punto de conexión privado es una interfaz de red con IP privada de una subred y debe estar en la misma región y suscripción que la red virtual, aunque el recurso de destino esté en otra región. Se necesita uno por subrecurso, es accesible desde redes emparejadas y desde local por VPN o ExpressRoute, y no bloquea por sí solo el acceso público. Las directivas de red habilitan NSG y UDR.
- Para crear un punto de conexión privado se indica la subred, el id. de recurso o alias, el subrecurso (group id) y el método de aprobación: automática con permisos sobre el recurso o manual, que queda Pendiente. La IP estática y el nombre de la interfaz de red solo se fijan al crearlo. Después se configura el DNS, por ejemplo con una zona privatelink vinculada a la red y un grupo de zonas DNS.
- Un punto de conexión privado solo envía tráfico cuando su conexión está en estado Approved; si quien lo crea no tiene permisos, queda en Pending hasta que el propietario lo apruebe. Las directivas de red están deshabilitadas por defecto en la subred: hay que habilitarlas para aplicar NSG o UDR, y la UDR debe ser al menos tan específica como el espacio de la red virtual para invalidar la ruta /32.
- Un servicio Private Link publica una aplicación que está detrás de un Standard Load Balancer, ligado a una configuración de IP de front-end y en la misma región que la red virtual. Antes de crearlo hay que deshabilitar privateLinkServiceNetworkPolicies en la subred. La visibilidad limita quién puede solicitar conexión, la aprobación automática evita aprobar a mano y TCP Proxy V2 revela la IP real del consumidor.
- Con un punto de conexión privado, el DNS público devuelve un CNAME al dominio privatelink y una zona DNS privada vinculada a la red responde con la IP privada, sin cambiar las cadenas de conexión. Usa los nombres de zona recomendados, una sola zona vinculada a todas las redes con clientes y un grupo de zonas DNS para que los registros se mantengan y se eliminen con el punto de conexión.

Design and implement service endpoints

- Un punto de conexión de servicio amplía hasta un servicio PaaS a subredes concretas sin cambios de DNS ni coste adicional: el tráfico va por la red troncal de Azure con IP privadas de origen. Si necesitas acceso privado desde el entorno local, desinstalar el punto de conexión público o protección contra la exfiltración por instancia, elige un punto de conexión privado.
- Los puntos de conexión de servicio se habilitan por subred con el nombre del recurso del servicio (Microsoft.Storage, Microsoft.Sql, Microsoft.KeyVault, ...), por ejemplo con az network vnet subnet update --service-endpoints. Al activarlos cambian las rutas de todas las NIC de la subred y pueden contarse conexiones TCP, en las rutas efectivas aparece el próximo salto VirtualNetworkServiceEndpoint.
- Una directiva de punto de conexión de servicio, asociada a una subred que ya tiene el punto de conexión Microsoft.Storage, permite solo las cuentas de almacenamiento enumeradas (por id. de cuenta, grupo de recursos o suscripción) y deniega todas las demás en cualquier región. Solo admite Azure Storage, no filtra el tráfico local y el secundario RA-GRS se permite solo.
- Para restringir un servicio a una subred con punto de conexión de servicio, establece la acción predeterminada en Deny y agrega una regla de red virtual; las reglas basadas en IP públicas dejan de coincidir porque el origen pasa a ser privado. El acceso local exige reglas de IP para las IP públicas de NAT, y el permiso joinViaServiceEndpoint es necesario en la subred.

5. Design and implement Azure network security services

15–20%

Implement and manage network security groups

- Un NSG contiene reglas con prioridad de 100 a 4096 que se evalúan de menor a mayor número hasta la primera coincidencia; no puede haber dos con la misma prioridad y dirección. Las reglas predeterminadas (como DenyAllInBound) no se eliminan, solo se invalidan. Los NSG tienen estado, evalúan IP privadas tras la traducción y los cambios solo afectan a conexiones nuevas.
- Un NSG se asocia a subredes e interfaces de red, siempre en la misma suscripción y ubicación que la red virtual. En entrada se evalúa primero el NSG de la subred y luego el de la NIC; en salida, al revés, y el tráfico debe estar permitido en ambos. Microsoft recomienda usar un solo nivel; az vm create crea un NSG en la NIC salvo que indiques --nsg "".
- Un grupo de seguridad de aplicaciones agrupa interfaces de red por función (web, lógica, datos) para aplicar reglas de NSG sin direcciones IP. Todas sus NIC deben estar en la misma red virtual que la primera agregada, su ubicación no se puede cambiar y no se puede eliminar mientras contenga interfaces. Se crea con az network asg create o New-AzApplicationSecurityGroup.
- Para asignar una interfaz a un ASG se configura en la configuración de IP de la interfaz de red, con az network nic ip-config update --application-security-groups o con Set-AzNetworkInterfaceIpConfig y Set-AzNetworkInterface. Una NIC puede estar en varios ASG de su misma red virtual y ubicación, y las reglas con ASG solo afectan a las NIC que son miembros.
- Las reglas de un grupo de seguridad de red se evalúan por prioridad (número más bajo primero) y la primera coincidencia detiene el proceso; las reglas predeterminadas no se eliminan, solo se anulan. En entrada se evalúa primero el NSG de la subred y luego el de la interfaz; en salida, al revés. Las reglas aumentadas combinan varios puertos e IP y las etiquetas de servicio y los grupos de seguridad de aplicaciones evitan mantener direcciones.

Design and implement Azure Firewall and Azure Firewall Manager

- Azure Firewall es un firewall con estado que ofrece reglas DNAT de entrada, reglas de red (IP, puerto, protocolo y, en Standard, FQDN mediante proxy DNS) y reglas de aplicación por FQDN para HTTP, HTTPS y MSSQL, además de etiquetas FQDN y de servicio, SNAT de salida e inteligencia sobre amenazas. No aplica reglas de aplicación al tráfico de entrada. Para filtrar HTTP/S entrante se usa Web Application Firewall.
- Azure Firewall tiene tres SKU: Basic ofrece filtrado con estado, NAT y FQDN de aplicación, pero la inteligencia sobre amenazas solo alerta y no hay proxy DNS ni FQDN en reglas de red; Standard añade proxy DNS, FQDN en reglas de red, categorías web y denegación por inteligencia sobre amenazas; Premium añade inspección TLS de salida y este oeste, IDPS y filtrado por URL completa. La inspección TLS de entrada corresponde a Application Gateway.
- Un diseño típico coloca Azure Firewall en AzureFirewallSubnet de la red central, con UDR 0.0.0.0/0 hacia su IP privada en los radios (sin propagación de rutas de puerta de enlace) y rutas en GatewaySubnet hacia el firewall para el tráfico local. La tunelización forzada exige la NIC de administración en AzureFirewallManagementSubnet, Standard y una tabla de rutas con 0.0.0.0/0 de tipo VirtualAppliance hacia la IP privada del firewall en las subredes de carga de trabajo. Los contadores az network firewall requieren la extensión azure-firewall. La NIC de administración puede habilitarse en un firewall existente deteniéndolo e iniciándolo.
- Para implementar Azure Firewall se crea AzureFirewallSubnet, el firewall y su configuración IP con una IP pública estándar y el SNAT hacia IP privadas se ajusta con los intervalos de IP privadas.
- En una directiva de Azure Firewall, las reglas se organizan en grupos de colecciones y colecciones con prioridades propias, pero siempre se procesan primero las DNAT, luego las de red y al final las de aplicación; las reglas son terminales. El tráfico que coincide con DNAT se permite sin pasar por reglas de red, las reglas de aplicación cubren HTTP, HTTPS y MSSQL, y sin coincidencia el tráfico se deniega.

Design and implement a Web Application Firewall (WAF) deployment

- Azure Web Application Firewall protege aplicaciones web frente a inyección SQL, XSS y otros ataques mediante directivas con reglas personalizadas (procesadas primero: IP, geografía, frecuencia, tamaño), conjuntos de reglas administrados (DRS/CRS en Application Gateway, Default Rule Set en Front Door) y Bot Manager, con exclusiones para falsos positivos. En Front Door Standard solo hay reglas personalizadas, las administradas requieren Premium.
- Al diseñar un WAF se elige Front Door para protección global en el perímetro o Application Gateway v2 para aplicaciones regionales y se asocian directivas globales, por sitio (agente de escucha) o por URL (regla basada en rutas), donde la más específica prevalece. Conviene empezar en modo de detección, ajustar con los registros y pasar a prevención, si Azure Firewall debe inspeccionar el tráfico a los back-end, Application Gateway va delante.
- El modo de detección solo supervisa y registra en los registros del WAF las solicitudes que coinciden con las reglas, sin bloquear; el modo de prevención aplica la acción y también registra. Con la puntuación de anomalías en prevención se actúa cuando la suma de gravedades llega al umbral, en Front Door la acción puede ser Block, Log o Redirect. Conviene empezar en detección, ajustar exclusiones y pasar después a prevención.
- En Front Door, los conjuntos de reglas administradas (Default Rule Set y Bot Manager) solo están disponibles en nivel Premium. Standard admite únicamente reglas personalizadas. El DRS 2.0 o posterior usa puntuación de anomalías e inspección cuerpos JSON, y permite exclusiones por regla, grupo o conjunto. Se pueden deshabilitar reglas o cambiar su acción, y las reglas personalizadas se evalúan antes que las administradas.
- Application Gateway WAF v2 ofrece CRS (Default Rule Set) basado en OWASP CRS con reglas de Microsoft Threat Intelligence, y versiones CRS anteriores: solo puede haber un conjunto basado en OWASP a la vez, pero se combina con el Bot Manager Rule Set. Las reglas se pueden deshabilitar o cambiar de acción, el DRS más reciente funciona por defecto en el nivel de paranoia 1 y las exclusiones evitan falsos positivos.