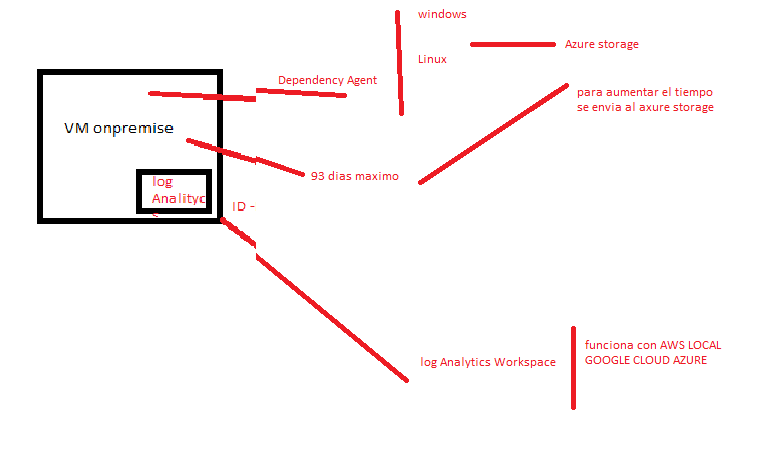
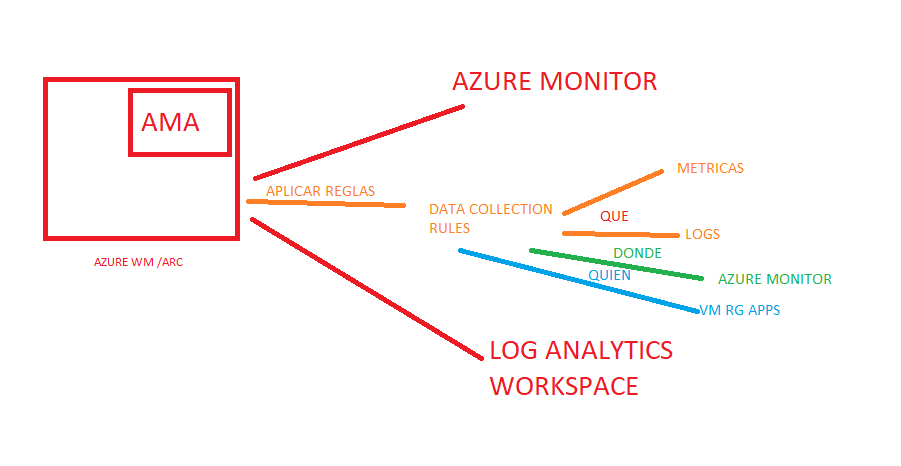
Azure Monitor : para vigilar el rendimiento de los recursos, supervisarlos y generar alertas tiene 4 funciones analizar (log analytics) visualizar (con workbooks conectados a azure sentinel , power bi, dashboard), responder (con escalamiento o alertas) integrar con logic app o evento hub

Event Hub: para transmitir e ingesta de grandes cantidades de datos en tiempo real

Logic Apps : para automatizar flujos de trabajo activándose con desencadenadores no code serverless y con conectores

Azure monitor tienes 2 variantes





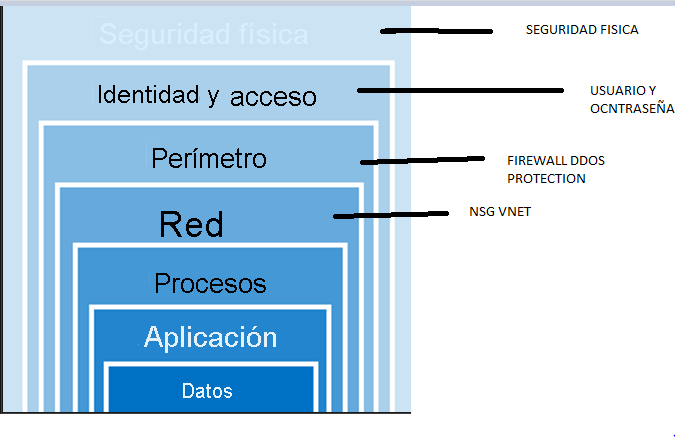
Azure sentinel

Solución SEIM Y SOAR escalable y nativa de la nube análisis de amenazas y seguridad

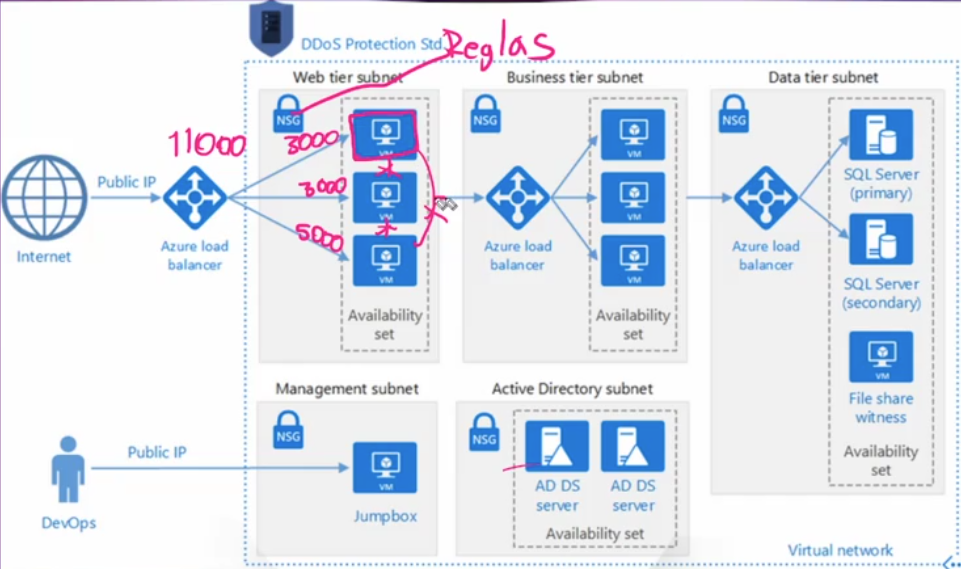
SIEM : SEGURITY INFORMATION AND EVENT MANAGEMENT te apila toda la información respecto a la seguridad

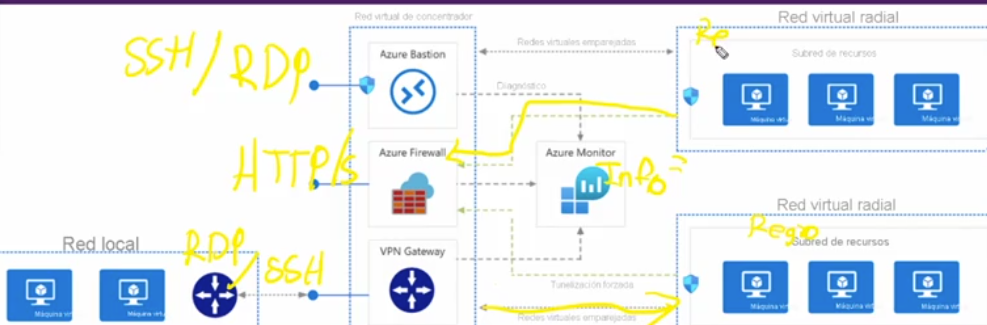
SOAR : SEGURITY ORCHESTRATION AUTOMATION AND RESPONSE respuesta automatizada de orquestación de seguridad usa la información del SIEM para responder a eso ataques

Recopila datos de seguridad de toda la empresa , detectar amenazas con amplia información sobre las mismas, responder rápidamente y automatizar la protección investigar incidentes guiados por IA

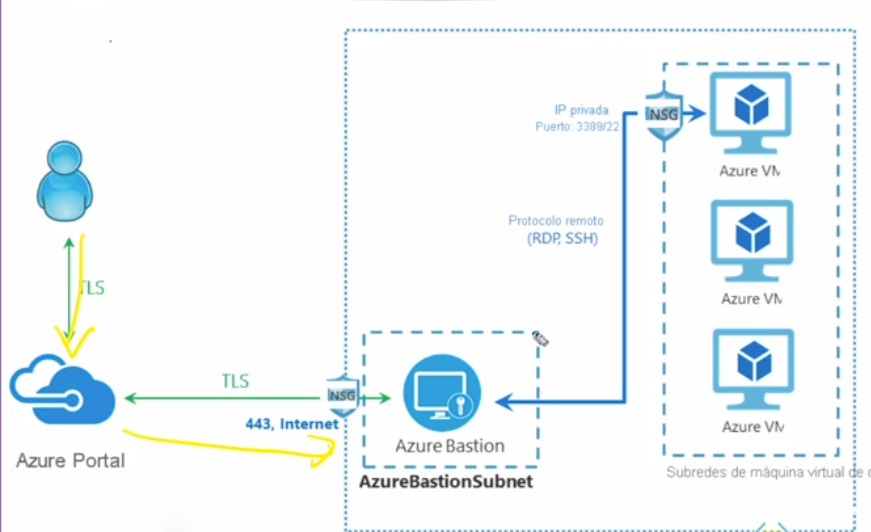
Microsoft Defender for Cloud

Es un recurso CSPM Y CWPP es decir maneja los eventos de seguridad y la seguridad





AzureFirewallSubnet -> es forzoso este nombre de identificador subnet



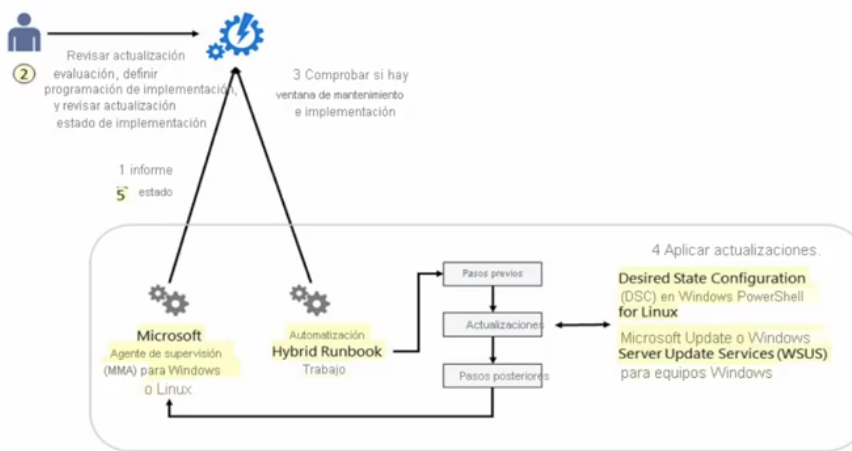
Una red virtual debe estar en la misma región por obligación Firewall si puede estar en otra región

Orden para crear Firewall

1 se crea la red virtual

2 se crea la subnet llamada AzureFirewallSubnet

3 después el Azure Firewall

Actualizar máquinas virtuales

Hay que instalar primero **Azure** Monitor Agent (**AMA)**