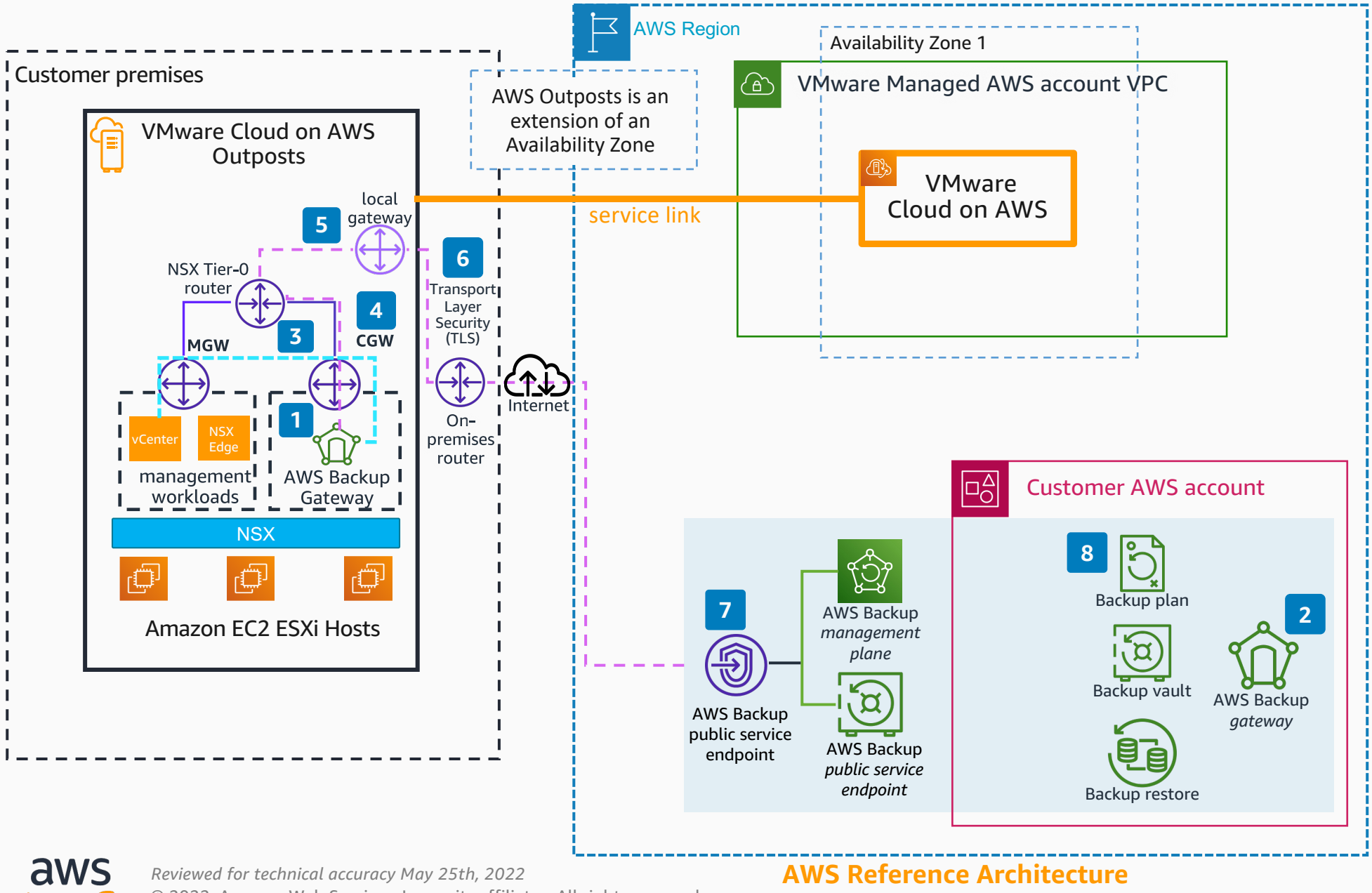
VMware Cloud on AWS Outposts with AWS Backup Integration

This architecture enables the customer to protect Virtual Machines (VM) running on VMware Cloud on AWS Outposts using AWS Backup.



1. The **AWS Backup gateway** appliance is available as a VMware virtual appliance that communicates with the vCenter and the **AWS Backup** public service endpoint for backup and restores. Deploy **AWS Backup gateway** in VMware Cloud on AWS Outposts vCenter on a customer-created network segment within the Software Designed Data-Center (SDDC).
2. Register **AWS Backup gateway** in the customer-owned AWS account where backup resources are managed. When the gateway is registered, add the vCenter to **AWS Backup** and associate with the gateway.
3. AWS recommends updating vCenter resolution to “Private DNS lookup” to keep the communication between vCenter and **AWS Backup gateway** private. This is optional; it is also possible to use this architecture with vCenter resolution to public domain name system (DNS).
4. **AWS Backup gateway** communicates with vCenter over the compute gateway (CGW).
5. **AWS Backup gateway** communicates with **AWS Backup** public service endpoints over the internet through the Local Gateway and the on-premises customer router.
6. The traffic from the **AWS Backup gateway** over the internet to the **AWS Backup** public service endpoints is encrypted using TLS.
7. The **AWS Backup** public service endpoint communicates with the **AWS Backup** management and storage plane through **AWS Backup** service endpoints. **AWS Backup** public service, the management plane, and the storage plan is managed by AWS.
8. Create and manage the backup plan and backup vault, assign virtual machines to the backup plan, view backups, and perform restores from the customer-owned AWS account.

AWS Reference Architecture

Reviewed for technical accuracy May 25th, 2022