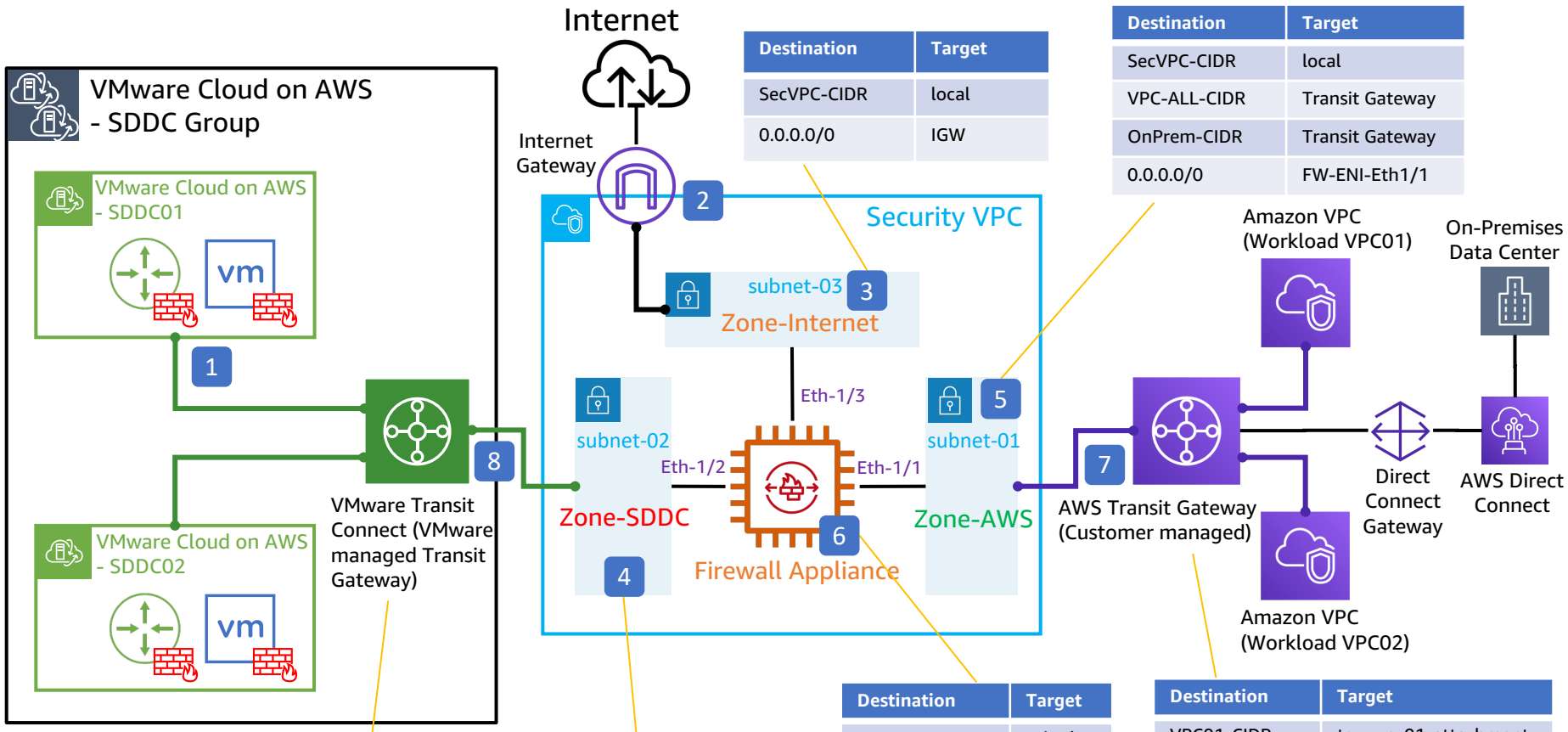
VMware Cloud on AWS – Security VPC Reference Architecture

Integrate third-party firewall appliances into VMware Cloud on AWS by leveraging the VMware Transit Connect.



Destination	Target
SecVPC-CIDR	local
0.0.0.0/0	IGW

Destination	Target
SecVPC-CIDR	local
VPC-ALL-CIDR	Transit Gateway
OnPrem-CIDR	Transit Gateway
0.0.0.0/0	FW-ENI-Eth1/1

Destination	Target
SDDC01-CIDR	vtgw-sddc01-attachment
SDDC02-CIDR	vtgw-sddc02-attachment
0.0.0.0/0	vtgw-secvpc-attachment

Destination	Target
SecVPC-CIDR	local
SDDC-ALL-CIDR	VTGW
0.0.0.0/0	FW-ENI-Eth1/2

Destination	Target
VPC-ALL-CIDR	Eth1/1
OnPrem-CIDR	Eth1/1
SDDC-ALL-CIDR	Eth1/2
0.0.0.0/0	Eth1/3

Destination	Target
VPC01-CIDR	tgw-vpc01-attachment
VPC02-CIDR	tgw-vpc02-attachment
OnPrem-CIDR	DXGW
SDDC-ALL-CIDR	tgw-secvpc-attachment
0.0.0.0/0 *(Optional)*	tgw-secvpc-attachment

1. Deploy a software-defined data center (SDDC) into an SDDC group. This automatically builds a VMware-managed Transit Gateway (VTGW) and establishes connectivity between SDDCs via the VTGW.
2. Build a security virtual private cloud (VPC) with access to the internet via an internet gateway (IGW).
3. Create one public subnet with access to the IGW and connect it to the firewall internet-bound elastic network interface (ENI). Network interface (Eth1/3) is assigned to an internet security zone (also called zone "Internet") within the firewall appliance.
4. Provision one private subnet that will be attached to the VTGW, with a dedicated route table to push all SDDC outbound traffic to the firewall interface (Eth1/2), which is assigned to a security zone for the SDDC group (Zone "SDDC").
5. Deploy another private subnet with a separate route table to be attached to the customer managed **AWS Transit Gateway** and the firewall interface (Eth1/1), which is assigned to a separate security zone for the AWS native side (Zone "AWS").
6. Provision a third-party (zone-based) firewall appliance within the Security VPC to provide transitive routing and policy inspection from zone *SDDC* to zone *AWS* and the *Internet* zone. "Source/Destination Check" must be disabled on all ENIs attached to the firewall. For internet access, source network address translation (SNAT) must be configured on firewall appliance to maintain route symmetry.
7. Create a new (or attach the existing) customer-managed **AWS Transit Gateway** to the Security VPC using subnet-01. This provides transitive routing between SDDCs and existing workload VPCs and on-premises data centers.
8. Attach the Security VPC to the VTGW using subnet-02. Configure a static default route at the VTGW towards the Security VPC attachment. All SDDC outbound traffic to the internet, and inbound access from the internet will be enforced to go through the firewall appliance within the Security VPC.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.