VMware Cloud Director | Tenant Security

Version Control
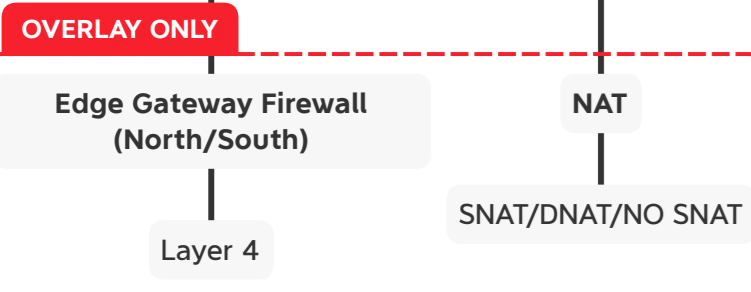
First release
by Abdullah Abdullah | VCDX #270   v1.0 based on VCD 10.2.2
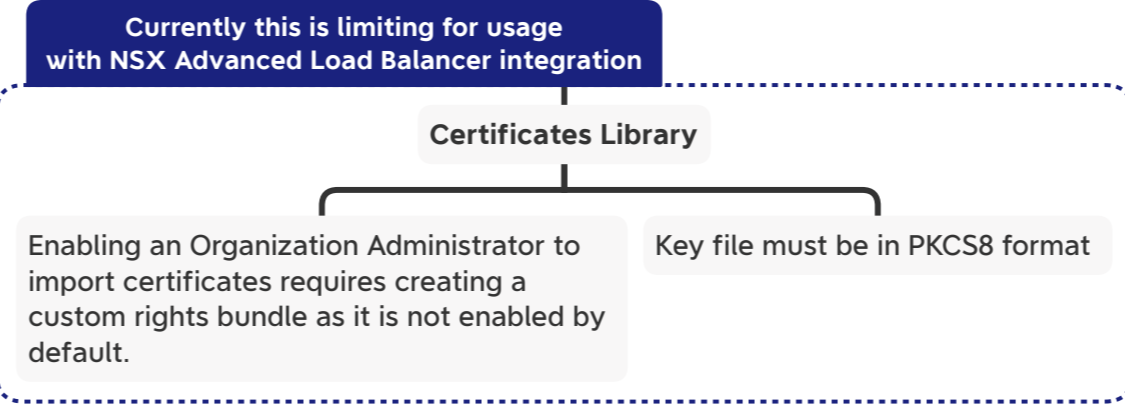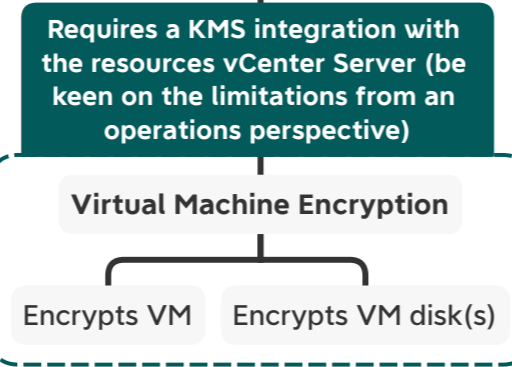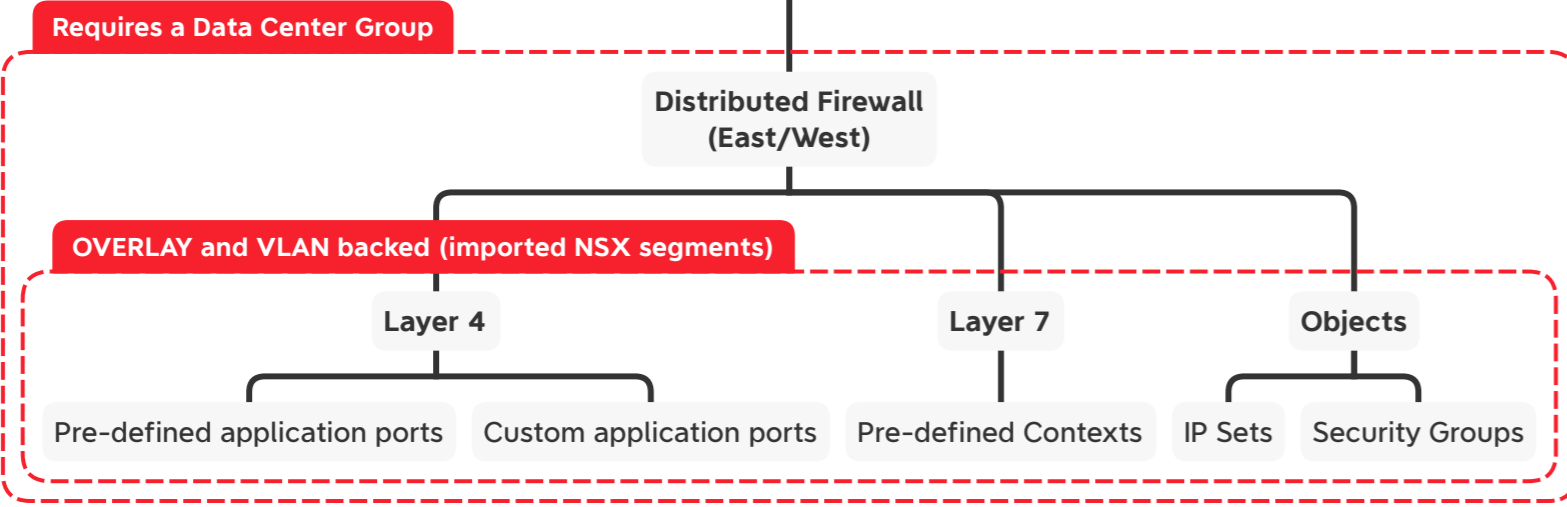
Tenant VDC(s) Security (Tenant Responsibility)

Edge Security

- **Edge Gateway Firewall (North/South)** — OVERLAY ONLY
  - Layer 4
- **NAT**
  - SNAT/DNAT/NO SNAT

OvDC Security

- **Distributed Firewall (East/West)** — Requires a Data Center Group
  - **OVERLAY and VLAN backed (imported NSX segments)**
    - **Layer 4**
      - Pre-defined application ports
      - Custom application ports
    - **Layer 7**
      - Pre-defined Contexts
    - **Objects**
      - IP Sets
      - Security Groups

Rule Specification
- Rule numbering, automatic with the ability to move rules up and down.
- Rule Name (Custom)
- State (Enabled/Disabled)
- Applications (Layer 4, pre-defined and custom)
- Context (Layer 7, only pre-defined)
- Source (IP Set / Security Group)
- Destination (IP Set / Security Group)
- Action (Allow/Deny)
- IP Protocol (IPv4 or IPv6 | IPv4 & IPv6)

Virtual Machine Encryption
Requires a KMS integration with the resources vCenter Server (be keen on the limitations from an operations perspective)
- Encrypts VM
- Encrypts VM disk(s)

Certificates Library
Currently this is limiting for usage with NSX Advanced Load Balancer integration
- Enabling an Organization Administrator to import certificates requires creating a custom rights bundle as it is not enabled by default.
- Key file must be in PKCS8 format

Tenant Portal Access (Service Provider Responsibility)

WAF
Its a good practice to direct administrators access to VCD via WAF to limit the vector of any internal compromise as well.
- SSL Termination — HTTP/API
- Passthrough — ConsoleProxy

Firewall
- Edge Firewall (Physical) — DNAT rules
- Data Center Firewall
  - NSX
  - Physical Firewall

Certificates
- WAF — Public CA Signed
- Internal Load Balancer — Public CA Signed (works as a safe switch in the even WAF fails then the NAT would be directed to the LB)
- KeyStore on Cells
  - HTTP/API — Private CA Signed
  - ConsoleProxy — Same Public CA Signed Certificate

Credentials
- Local — Limited policies
- LDAP — Follows credential provider policies (i.e. Active Directory Domain Services group policies)
- Enhanced with 2FA
  - SAML
  - OAuth2

System Logging
- NSX-T and ESXi hosts must be configured so that to get tenant edge and DFW logs.
- VCD Cells should be configured to send the logs to a syslog server (vRLI agent as an example). — Audit Messages needs to be explicitly configured to be sent to a syslog host (via Cell Management Tool).
- SNMP Agent — Support v1, v2c or v3 — v3 provides enhanced security

Compliance
- FIPS mode
  - Disabled by default.
  - Mind the limitations opposed by enabling FIPS (check installation and configuration guide).
- List of Allowed SSL Ciphers — Via Cell Management Tool (CMT)

General System Settings (options that should not be kept as default and must be configured based on requirements)
- Activity log history to keep
- Activity log history shown
- Default syslog server settings for networks
- Idle session timeout
- Maximum session timeout
- Verify vCenter and vSphere SSO certificates
- Verify NSX Manager certificates
- Number of resource intensive operations running per user
- Number of resource intensive operations to be queued per user (in addition to running)
- Number of resource intensive operations running per organization
- Number of resource intensive operations to be queued per organization

Cloud Director Appliances Patching
- Application patching (per VMware releases and advisories).
- Photon OS patching
  - This can be done via TDNF
  - Mind this KB (https://kb.vmware.com/s/article/2090839)
  - Keep GSS involved
  - Perform patching and upgrades in a staging environment is the ONLY common sense prior to applying to production (don't let any savings in the budget tell you otherwise).