

Ottobre 12, 2022

# NSX V2T

## Storia di una migrazione complessa





GIOVANNI DOMINONI  
VMware System Administrator

# Bio

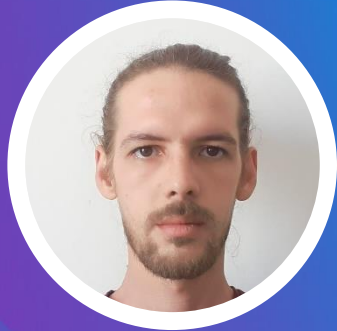
- **VMware System Administrator e VMware Specialist VCP-DCV, VCP-NV, VCIX-DCV, VCIX-NV, vSAN Specialist** presso Value Transformation Services
- VMware Academy Instructor e architetto dei contenuti e dei laboratori vSphere presso eForHum
- Nel tempo libero cerco di divulgare argomenti relativi a VMware attraverso il mio blog
- vExpert, vExpert NSX e vExpert PRO
- Board Member VMUG Italia



Linkedin: <https://www.linkedin.com/in/giovanni-dominoni-65065678/>

Twitter: [@Giodomi1989](https://twitter.com/Giodomi1989)

Blog: <https://www.giovannidominoni.it/>



ALBERTO STANI  
Network Architect

# Bio

- Laurea in Electronics and Telecommunication Engineer presso Università degli studi di Trento
- Network Engineer in Kyndryl , a supporto di Value Transformation Services
- SDN Architect a supporto di Value Transformation Services

Linkedin: <https://www.linkedin.com/in/alberto-stani-b13171b7>

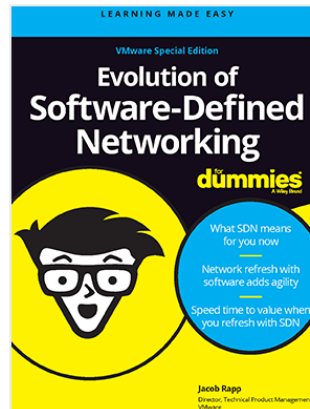
Mail to: [stanielberto@gmail.com](mailto:stanielberto@gmail.com)

## SDN e NSX

SDN sta per Software Define Network ed è un approccio al network che utilizza programmazione software per indirizzare il traffico e comunicare con l'infrastruttura fisica.

In poche parole SDN è la trasformazione in software di quelli che sono i principali device network: **router, switch, firewall e load balancer**.

Ciò comporta notevoli vantaggi nella gestione e nella flessibilità, aumentando al contempo la sicurezza utilizzando il modello a microsegmentazione Zero Trust.



<https://www.vmware.com/it/topics/glossary/content/software-defined-networking.html>

# Agenda

- Introduzione
- Design di NSX-V
- Opzioni di Migrazione
- Design di NSX-T
- Preparazione / Assessment
- Tools Utili
- Piano di Migrazione
- Migrazione
- Q/A

# Introduzione

Storia della migrazione del Private Cloud di un noto Istituto Bancario Europeo

Da NSX-V a NSX-T, tramite custom tools e un approccio “alla Carta”

Grazie al supporto di VMware PSO e 27Virtual

Numeri alla mano:

+3K Virtual Machines , +15K Regole Firewall , +10K Ipsets

12 ESGs , 4 DLRs , +50 Segments

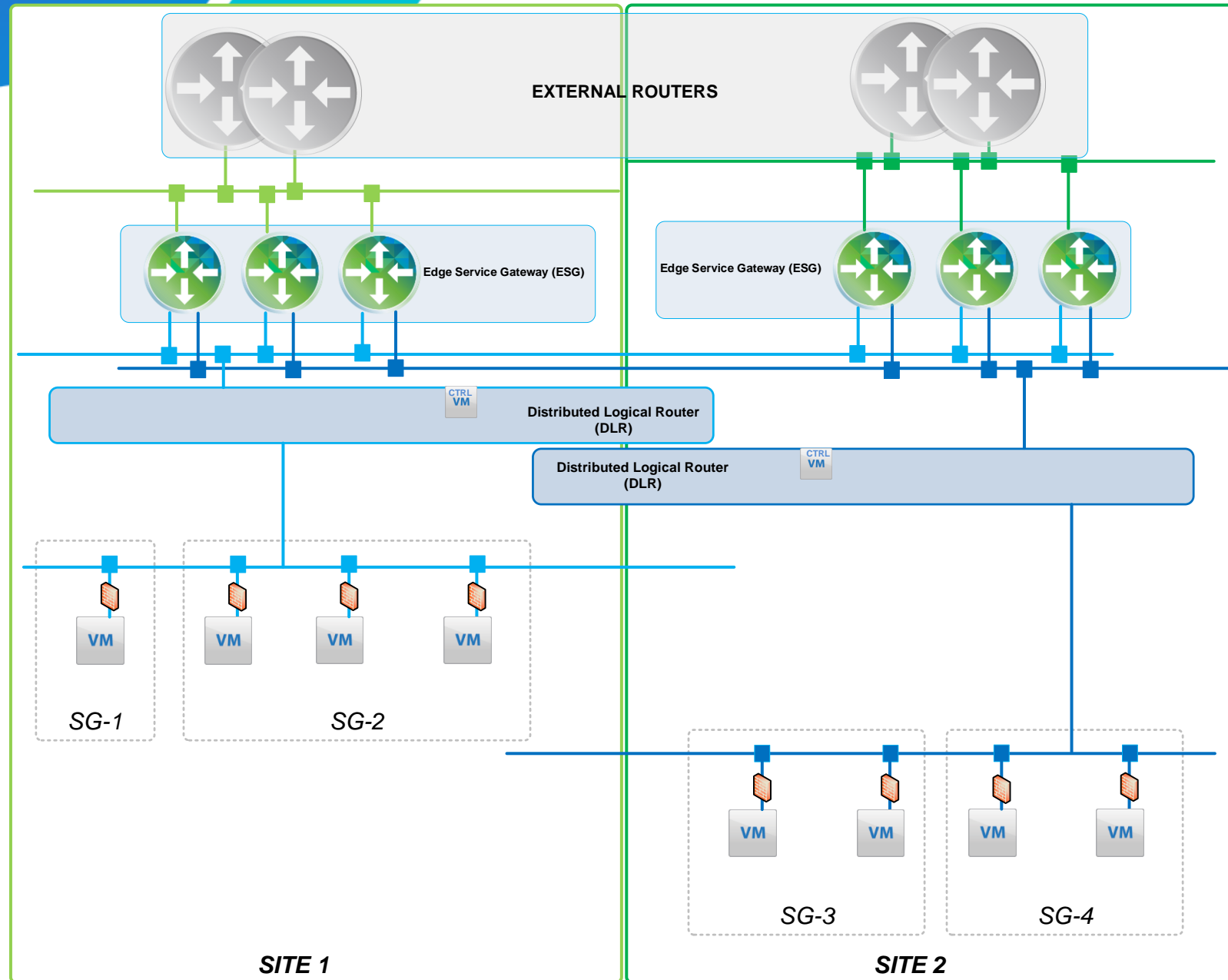
# NSX-V DESIGN

## Architettura Network:

- Multisito Active / Active
- Datacenters in DR
- Singolo NSX Manager
- Singolo Vcenter
- NSX Edge/Management Cluster Dedicato
- Cluster workload singolo sito e stretched

## Security:

- Modello 0 Trust Security
- Security Group con Tag Membership
- Regole tra Security Group (E/W)
- Regole tra Security Group e Ipset (N/S)
- Creazione via Automation Regole DFW via API



## V2T OPZIONI DI MIGRAZIONE

Le possibilità di migrazione V2T sono principalmente tre:

### CONVERSIONE

Migrazioni automatizzata di un ambiente NSX-v in NSX-T tramite il Migrator Coordinator o soluzioni terze parti

### Co-EXISTENCE

Nuovo ambiente NSX-T, in parallelo al esistente NSX-V

### LIFT e SHIFT

Migrazione del Workload di produzione da NSX-V a NSX-T  
Tramite piano di migrazione ad-hoc

Requisiti della nostra migrazione:

- Hot migration No VM or Service downtime
- No Big bang, limitare il rischio e procedere con gruppi di migrazione
- No Security deviation, 0 Trust model da mantenere
- Rollback possibile in ogni momento



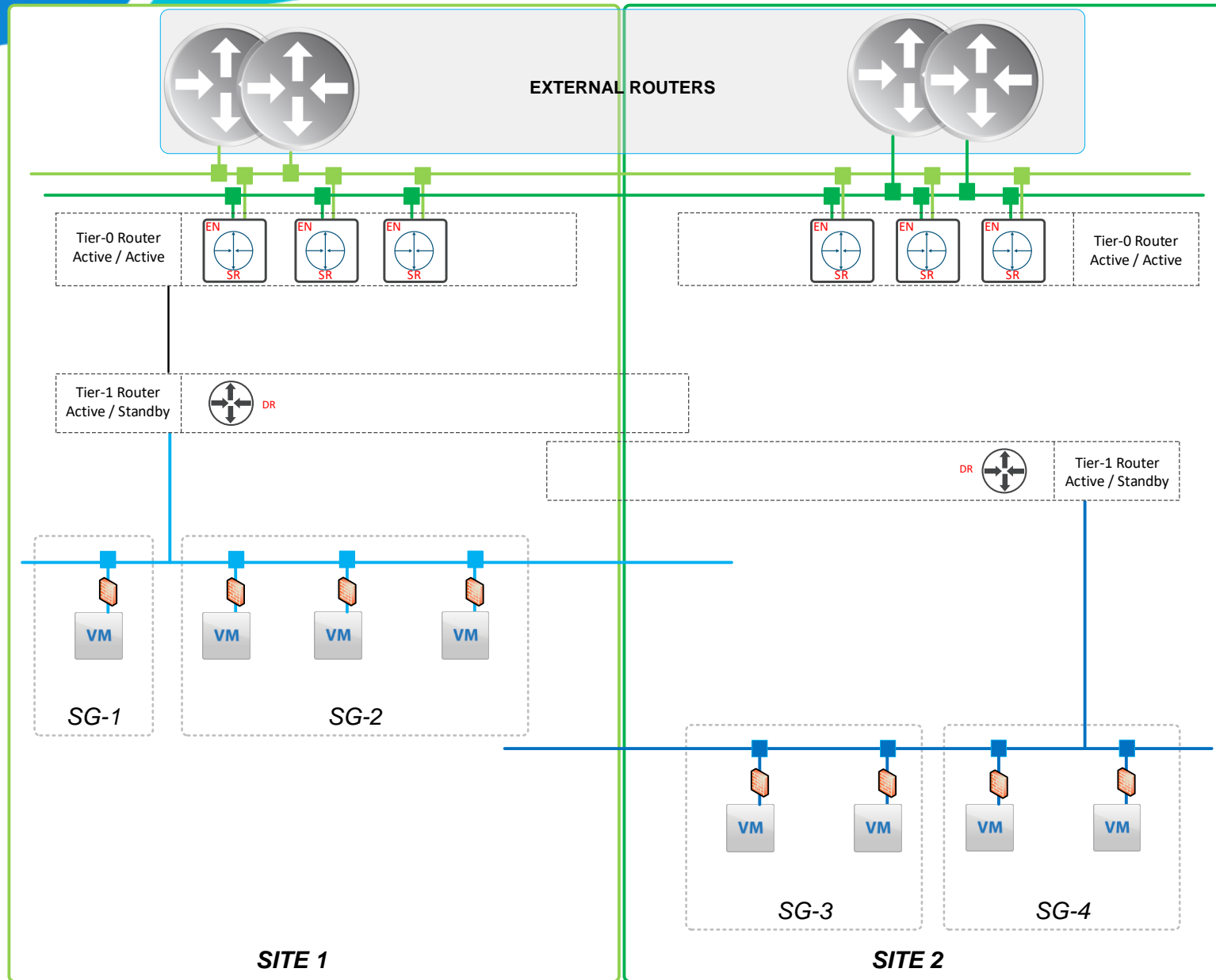


# NSX-T DESIGN

L'ambiente su cui migrare è un ambiente NSX-T realizzato all'interno dello stesso vCenter ma che deve mantenere e migliorare quanto ottenuto con NSX-V

## Architettura "T":

- T0 Edge Cluster dedicato per ogni sito
- 3 T0 Nodes per Site, in Active/Active mode
- T1 in Routing mode, solo componente distribuita
- Configurazione BGP custom per forzare traffico sul sito "primario"
- Edge Node Failover, in caso di DR, tramite Vmotion e BGP "tricks"
- Edge e Workload Clusters separati, come in "V"
- Singolo VDS per management e overlay networks



### Finding Principali

- Ambiente complesso Multi-Site, requisiti di migrazioni non compatibile con soluzioni standard
- Clean-up raccomandato/necessario

### Rimozione regole DFW non utilizzate

- Estrazione tramite RestNSX e VRNI per determinare quali regole non sono utilizzate (“Hit Count”)
- Analisi Regole “Shadow” / Doppie (**vrni query**: “firewall rules where Alert = 'Firewall Rule Masked Alert”)
- Pulizia delle regole non utilizzate e Shadow ha diminuito del 25% le regole totali nel DFW

### Verifica della compatibilità del DFW

- Sezioni DFW con meno di 1000 regole
- Numero Oggetti per regola
- Verifica e trasformazione servizi non compatibili con NSX-T – M.A.T

### Applied-To

- L'utilizzo dell'Applied To per limitare l'utilizzo di regole “solo dove necessario”
- Analisi del numero di FW rules per host

### Test multipli e validazione

- Porting della configurazione DFW da PROD a TEST, per emularne la complessità (RESTNSX)
- Più round per simulare la migrazione e “scoprire” eventuali problematiche o possibili ottimizzazioni (RESTNSX M.A.T)

# TOOLS UTILI

## RESTNSX

Con RestNSX è possibile analizzare l'ambiente NSX-v prima della migrazione andando e pulire gli oggetti non utilizzati  
<https://restnsx.com/>

## IP-Set Injection

Per far comunicare gli ambienti "V" e "T", durante la migrazione, è necessario iniettare "Ipsets temporanei"  
Tramite custom script o l'utilizzo di RESTNSX M.A.T

## Migrazione del DFW - RESTNSX M.A.T

M.A.T in questo caso specifico è un tool fenomenale in grado di salvare la configurazione del DFW di NSX-V e riportarla correttamente sul DFW di NSX-T  
E' in grado di generare report, effettuare rollback e di applicare i TAG alle macchine migrate in "T", tramite I Post Migration Tasks  
<https://restnsx.com/mat/>

## NSX-T Bridge

Gli EDGE Bridge di NSX-T hanno permesso l'estensione di network Logical Switch NSX-v su NSX-T eliminando ogni possibile downtime  
[https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt\\_31\\_migrate.pdf](https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_migrate.pdf) - pag.107

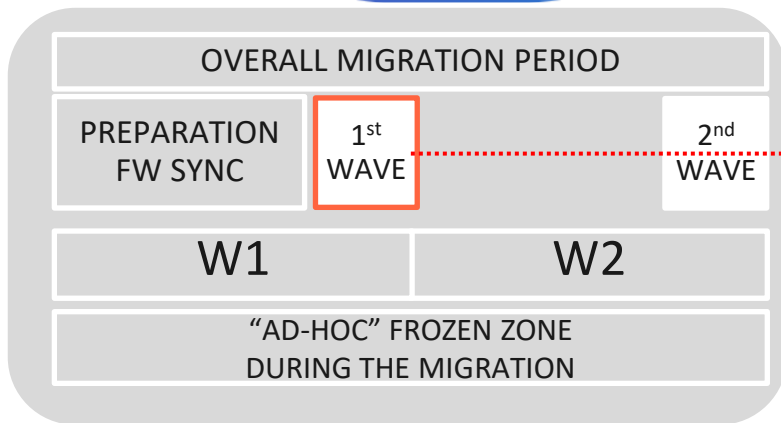
## vMotion Script

Script sviluppato "in casa" per poter gestire la migrazione massiva di VMs, in waves, tra Clusters ed eventuale RollBack

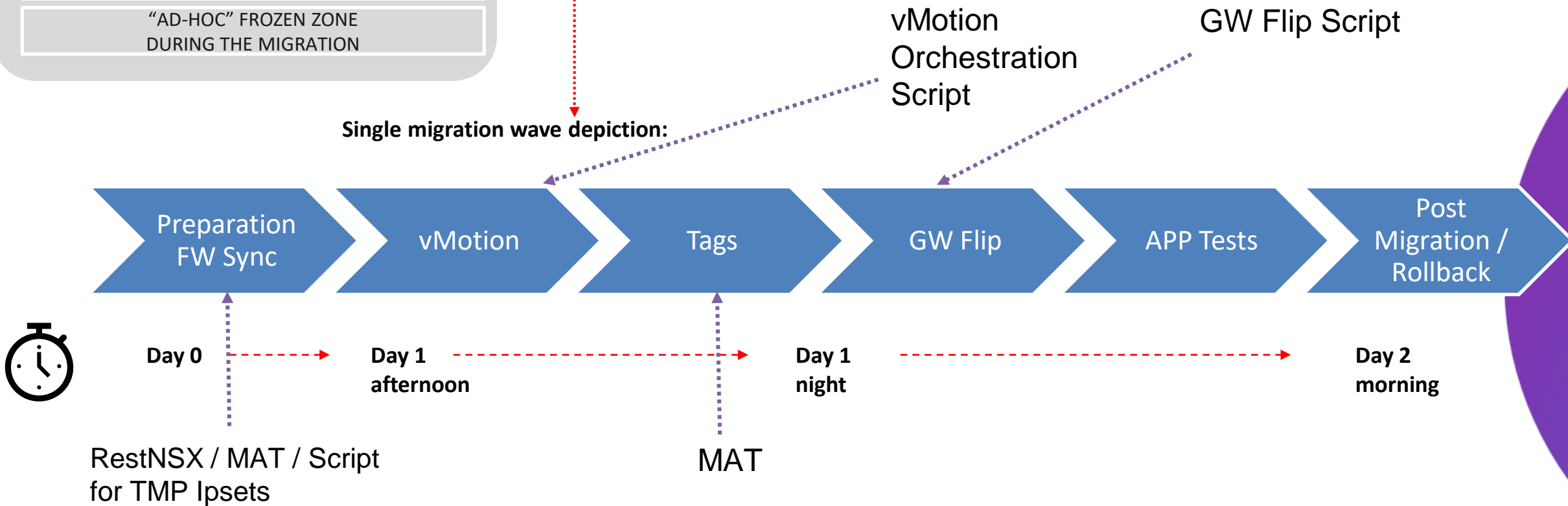
## Script i per Gateway flip

Custom Script per migrare il Gateway di ogni network da NSX-V a NSX-T  
Pochi secondi di disconnessione, unico downtime della migrazione

# PIANO DI MIGRAZIONE

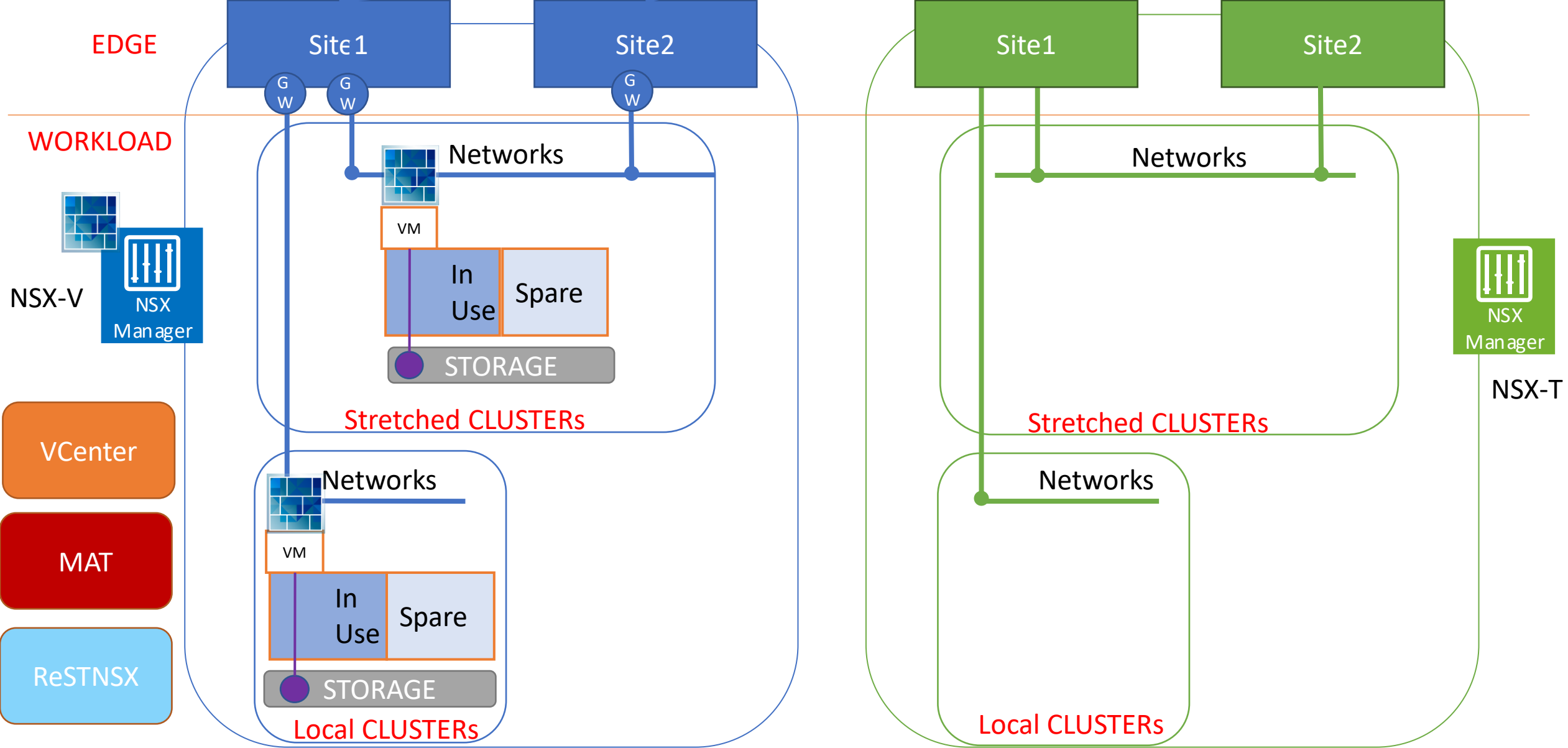


Single migration wave depiction:



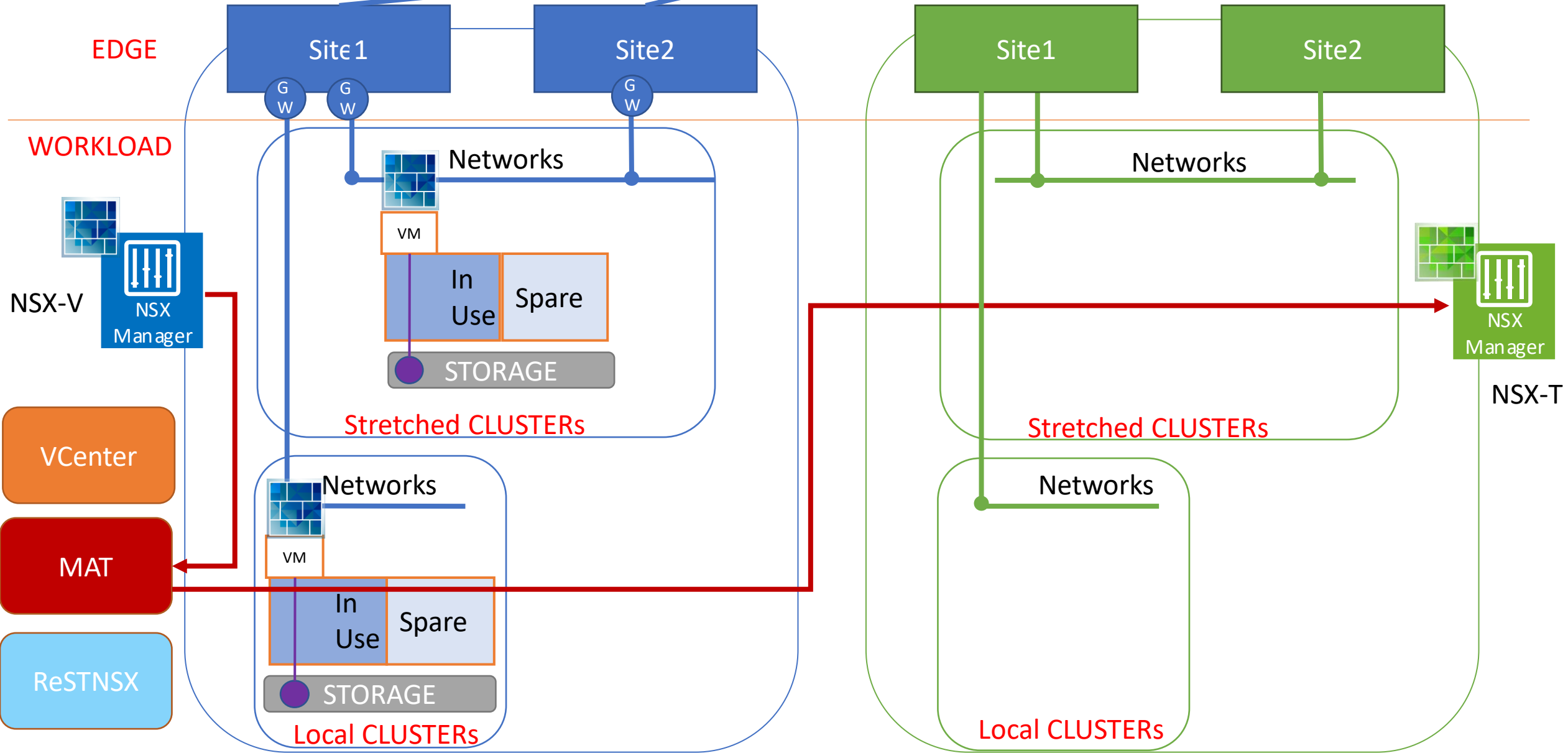
NSX-V Private Cloud  
&  
NSX-T Green Field

Physical Network



# PREPARAZIONE MAT Replica V2T

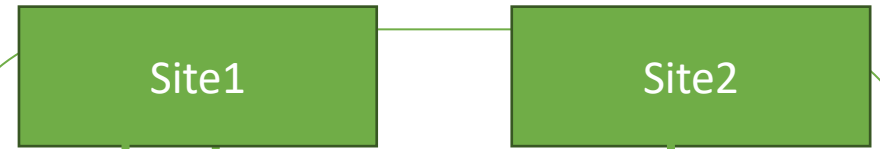
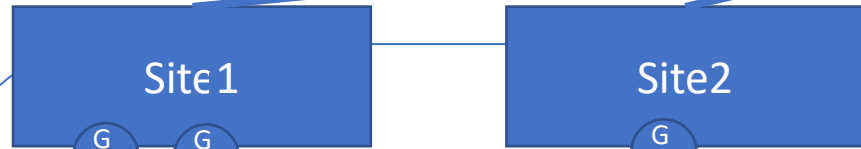
Physical Network



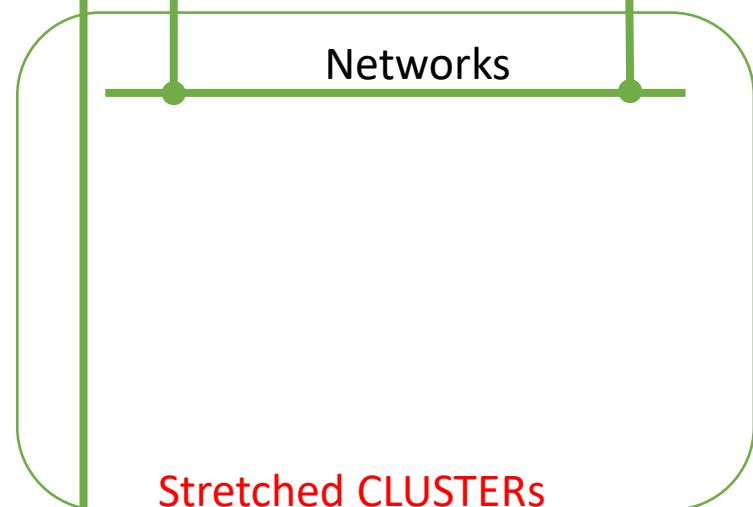
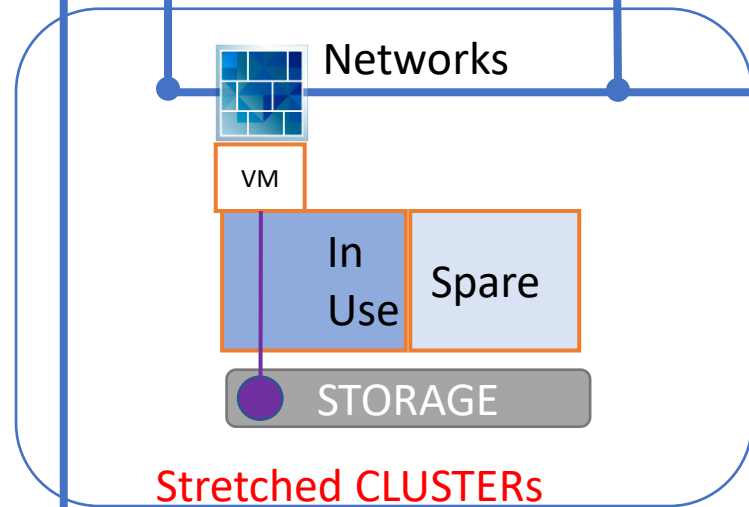
**PREPARAZIONE**  
Bridges e Hosts

Physical Network

EDGE



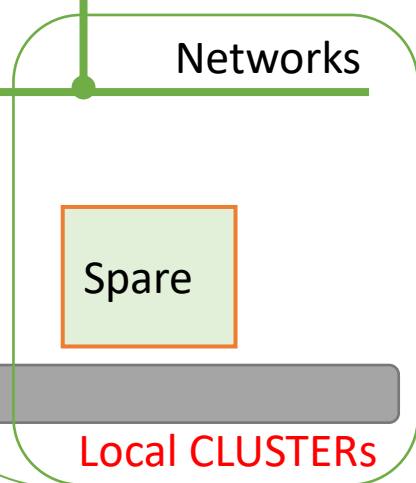
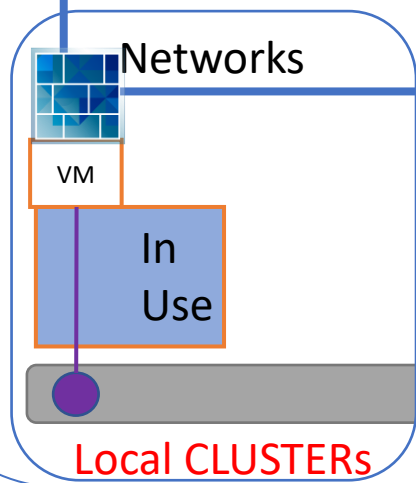
WORKLOAD



VCenter

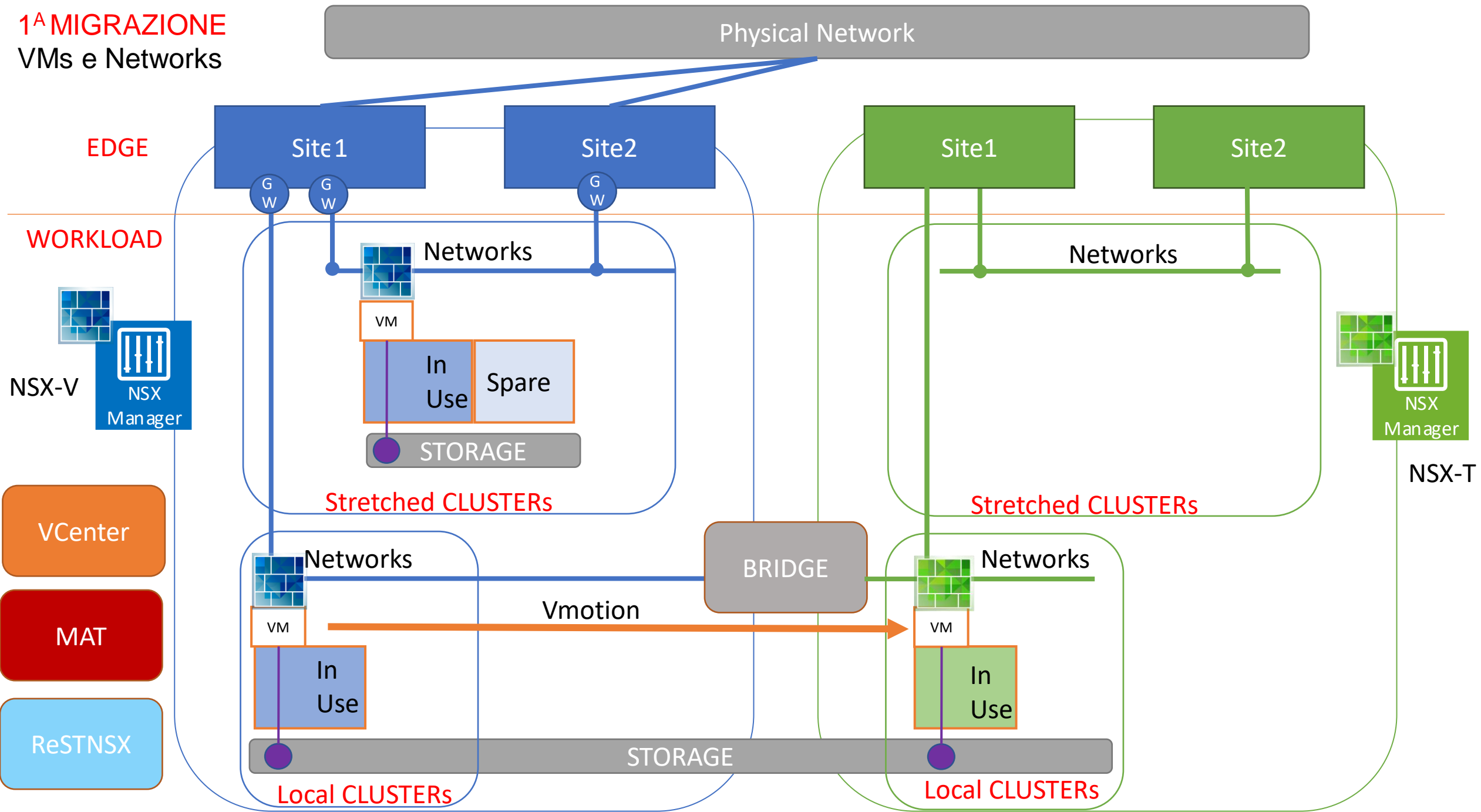
MAT

ReSTNSX



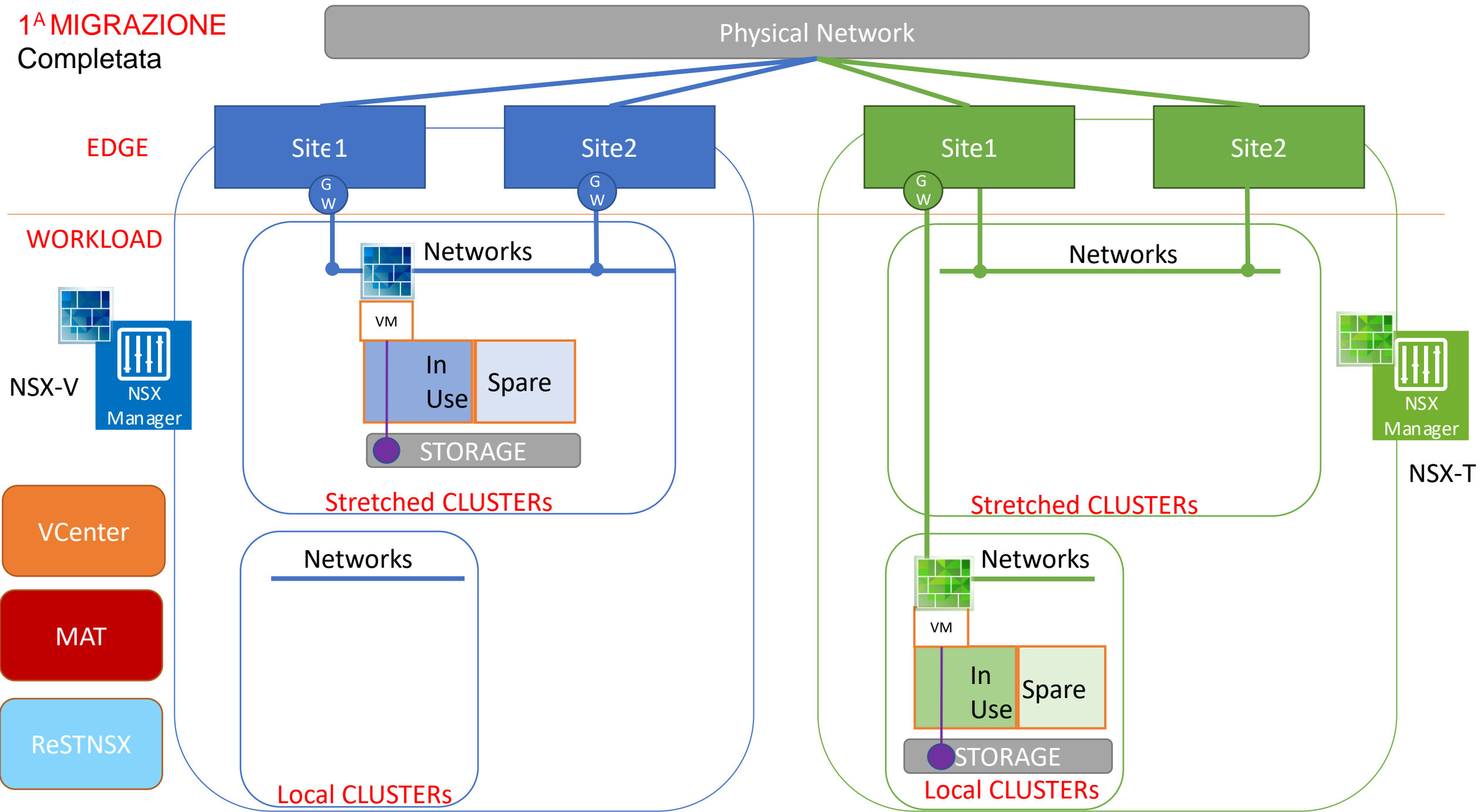
NSX-T

# 1ª MIGRAZIONE VMs e Networks

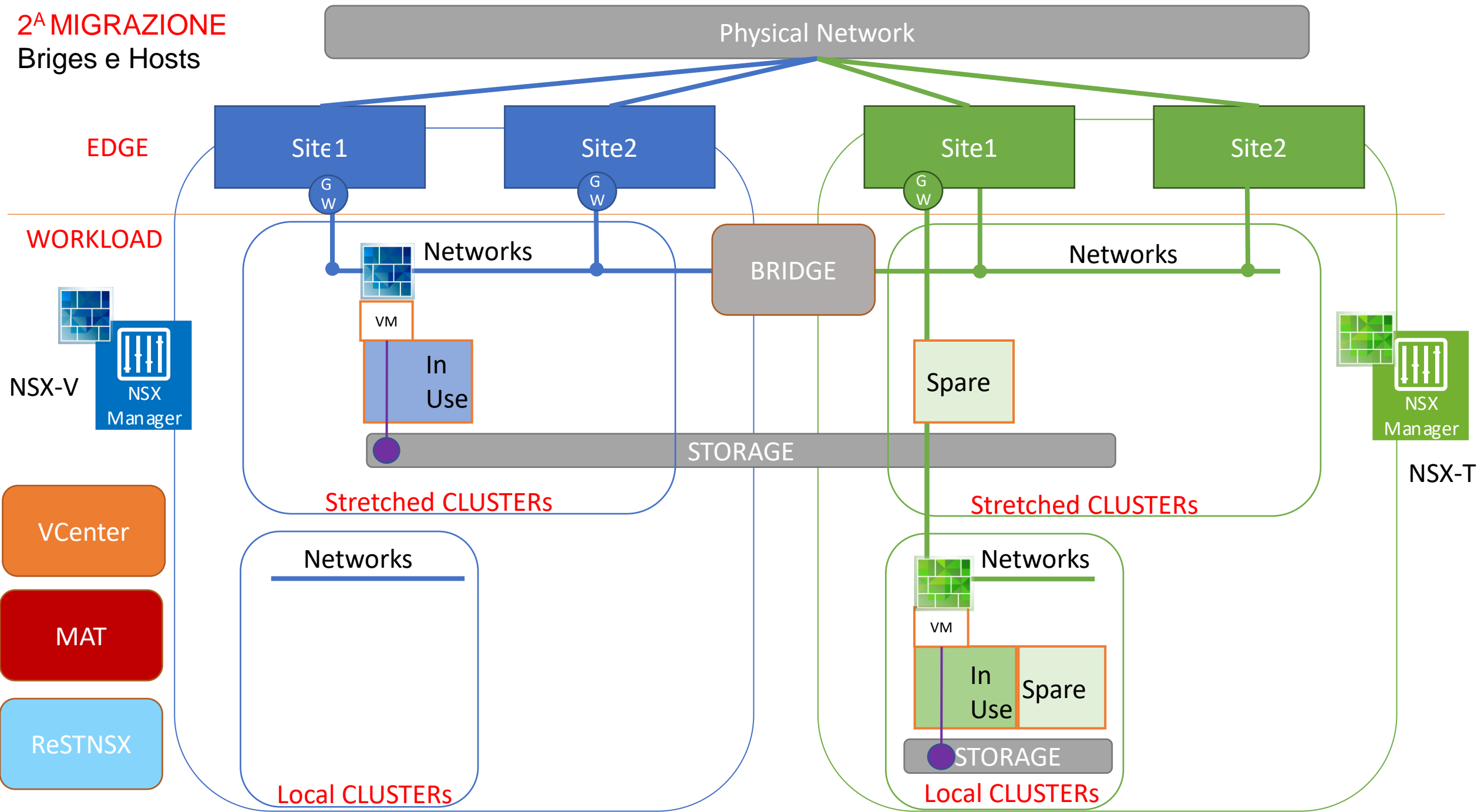




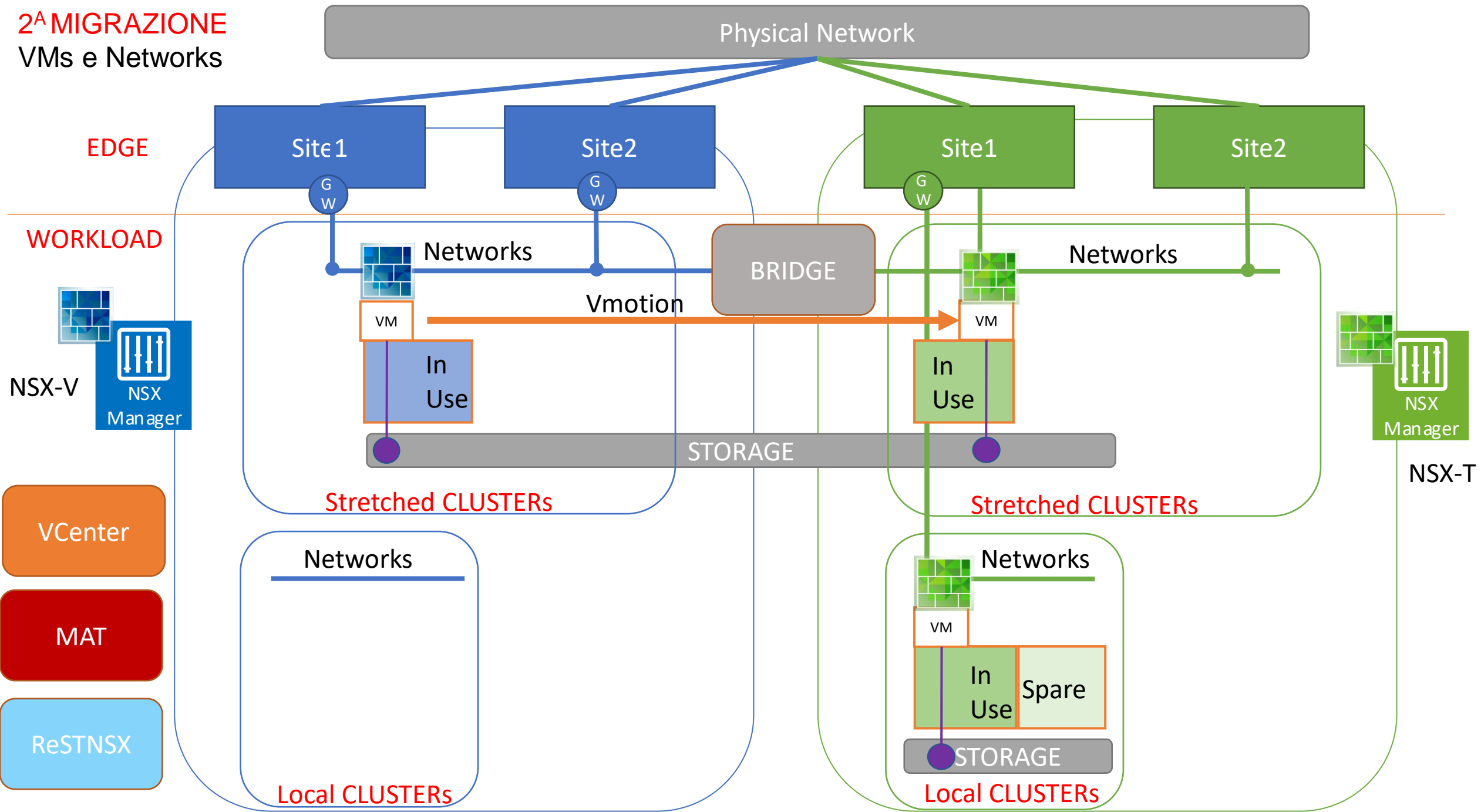
# 1<sup>A</sup> MIGRAZIONE Completata



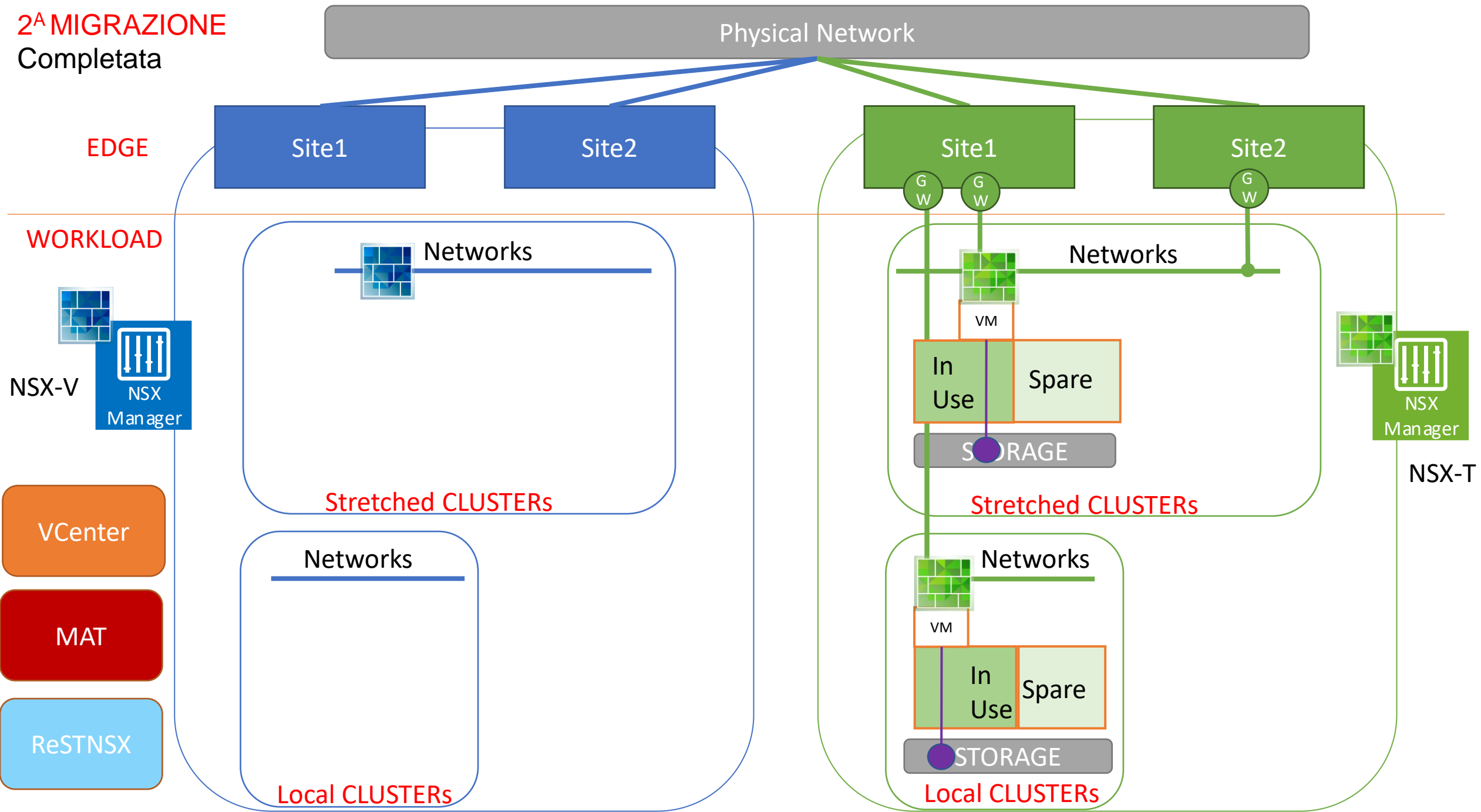
# 2<sup>A</sup> MIGRAZIONE Briges e Hosts



# 2<sup>A</sup> MIGRAZIONE VMs e Networks



# 2<sup>A</sup> MIGRAZIONE Completata



## CONCLUSIONE

# Grazie!

Menzioni Speciali:

- 27Virtual Team / Chris Cooke
- RestNSX / DJ Antinucci



Q/A



113 Seaboard Lane, Suite C-250, Franklin, TN 37067

# BACKUP



113 Seaboard Lane, Suite C-250, Franklin, TN 37067

