

Securing your Data Center with NSX-T Microsegmentation

Anandit Gupta & Nisheeth Kumar Khemka

Table of Content

— 03

1. Introduction

— 03

2. Challenges with traditional firewalls

— 05

3. Capabilities

— 06

4. NSX Firewall design

— 07

5. VM tagging

— 07

6. NSX-T security policies enforcement order

— 08

7. Customer use case

7.1 Process workflow

7.2 Tools used

7.3 Phases per application

7.4 Documents preparation per application

7.5 Automation tasks performed

7.6 Benefits

7.7 Key challenges

1. Introduction

The landscape of the modern data center is rapidly evolving. The shift towards virtualized workloads, software-defined data centers, multi-cloud landscapes, and new architectural models like micro-services and containers are driving constant evolution. New applications are being rolled out so quickly that the old security systems can't keep up anymore. This makes it harder to stay safe.

The older applications were monolithic stacks where infrastructure and applications were aligned, and the traditional firewalls were built to support those architectures. Now the applications have become distributed systems, and the older security policy doesn't work well with the new system, which makes data protection complicated. The security silos created using unrelated approaches makes it hard to predict and manage overall company security risks.

2. Challenges with traditional firewalls



Network topology dependency

The traditional physical appliance firewalls are network topology dependent and hence, filtering can only be applied at the network boundary for North-South traffic (client to server) and not for East-West traffic (server to server).



Hair pinning of traffic

All traffic needs to be sent to centrally hosted traditional firewall / IPS appliances which leads to hair pinning. This makes the appliance firewall a network chokepoint leading to application latency and unnecessary use of network bandwidth.



Blind spots

The legacy approach is incapable of detecting intra-host or intra-vlan traffic. There are challenges of vendor software backdoor (analytics, support, collection) and legacy end-of-support OS. All these flows do not have visibility or firewalling.



Unable to dynamically scale

There is no dynamic scaling of applications or workloads as it is dependent on physical firewall capacity. The solution is to upgrade current appliances or add newer appliances to accommodate the growing need of business and data centers leading to an increase in CaPex.



Only broader segmentation

With traditional firewalls, only broader network segmentation can be performed. There are no options for granular application and micro-segmentation to protect organizations from East-West lateral movement within the data center.



Static policies

There is no option to add dynamic workload context-based policy as it only allows to define the security policy based on IP or gateway Interface.

A foundational aspect of addressing this problem is the implementation of micro-segmentation. NSX is a networking and security platform able to deliver micro-segmentation across all the evolving components comprising the modern data center. NSX-based micro-segmentation increases the agility and efficiency of a data center while maintaining an acceptable security posture. VMware NSX Micro-segmentation meets the security requirements needed to provide effective security controls and risk management within the modern data center by operationalizing agile security.

With the exponential increase in East-West traffic, the ideal solution to complete data center protection is to protect every traffic flow inside the data center with a firewall, allowing only the flows required for applications to function. This is known as the Zero Trust Model.

HCLTech observes similar challenges while working with customers running on legacy infrastructure with traditional firewall and leverages the capabilities provided by NSX-T micro-segmentation.



3. Capabilities



Distributed, granular enforcement

It provides distributed and granular enforcement of security policies to deliver protection down to the workload level, eliminating the need for network changes.



Scalability and throughput

The Service-defined Firewall is elastic, with the ability to auto-scale as workloads spin up or down due to its distributed nature.



Intra-application visibility

It automatically determines the communication patterns across all types of workloads, makes security policy recommendations based on those patterns, and checks that traffic flows to confirm the deployed policies.



Declarative API

With the NSX Service-defined Firewall, security teams can move at the speed of development to deliver a true public cloud experience on-premises using automation scripts / tools.



Advanced threat prevention

Security teams can easily deploy advanced threat prevention capabilities such as distributed IDS/IPS, network sandboxing, and network traffic analysis/network detection and response (NTA/NDR) to protect against known and zero-day threats.



Micro-segmentation and cyber security standards

NSX is the only micro-segmentation solution to have achieved the following industry standards:



- 1
Common criteria certification
- 2
FIPS 140-2 certification
- 3
ICSA labs certified firewall
- 4
Satisfies all NIST cybersecurity recommendations for protecting virtualized workload
- 5
Validation in a published micro-segmentation cybersecurity benchmark report by Coalfire

4. NSX Firewall design

The NSX Firewall design includes two types or layers of firewalls.



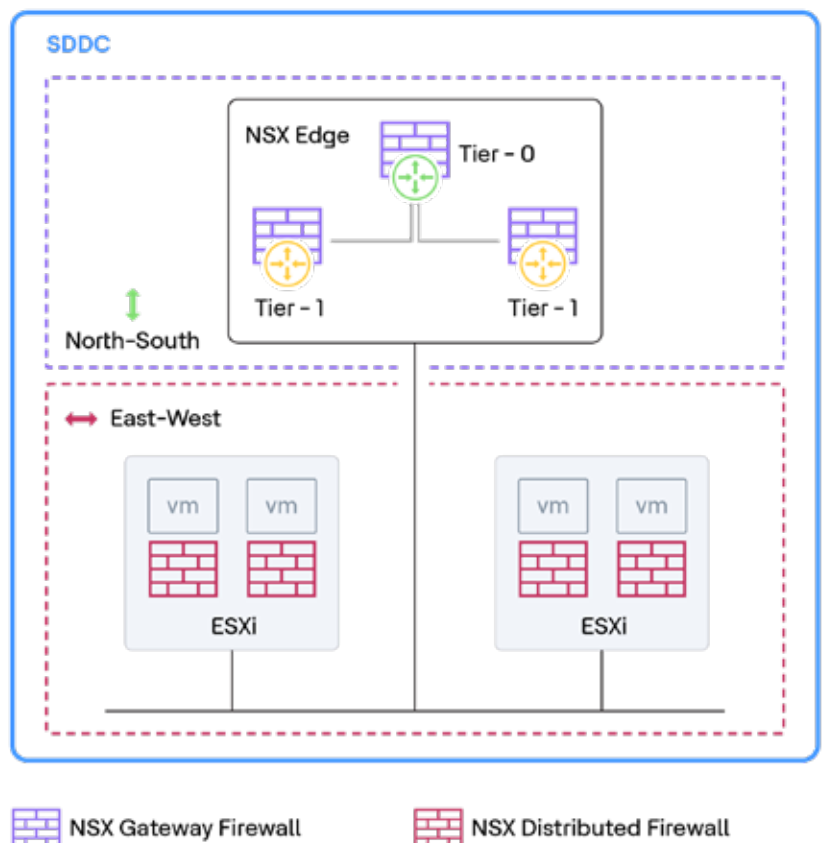
Gateway firewall

North-South Firewalls that are designed to protect the SDDC's perimeters or boundaries.



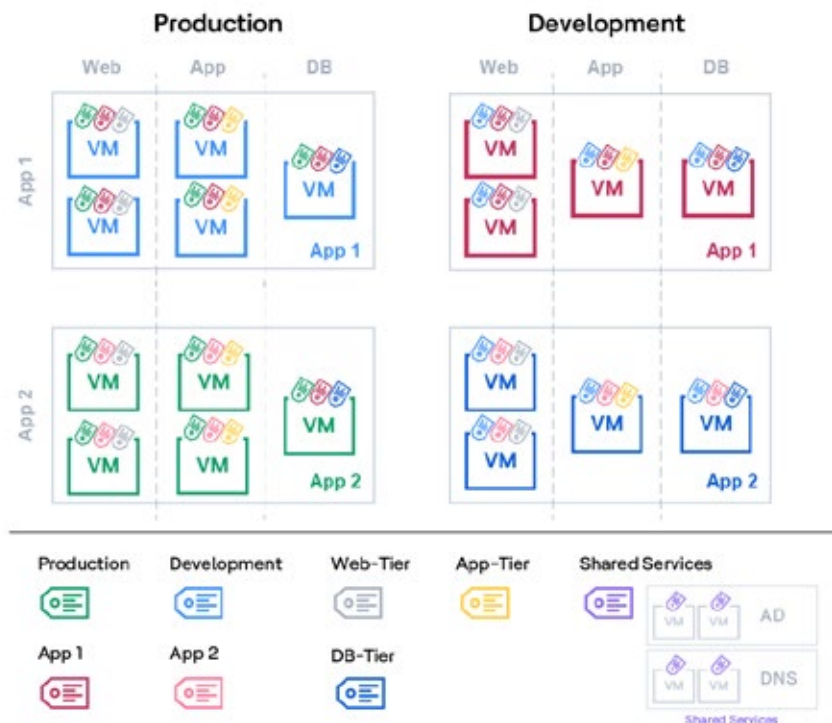
Distributed firewall

East-West Firewalls that protect workloads at the vNIC level.



5. VM tagging

Security Tags are applied to Physical Servers, Virtual Machines, Logical Ports, and Logical Segments and can be used for dynamic Security Group membership. NSX allows multiple tags per VM allowed, up to 30 to identify environment, zone, tenant, application, tier, OS, etc. The example shown below depicts the tags assigned to VM based on environment (Production or Development), App Name (App-1 or App-2), Tiers (Web or App or DB). These tags can be utilized to update security groups dynamically.



HCLTech recommends assigning tags to VMs and leveraging the dynamic grouping of objects based on group definition by matching the tags. This helps in automatic group update and policy applied to similar VMs without additional efforts.

6. NSX-T security policies enforcement order

All rules are processed left to right under the distributed firewall category (Ethernet -> Emergency -> Infrastructure -> Environment -> Application) and from top to bottom within the section.



Each rule is checked against the top rule in the rule table before moving down the subsequent rules in the table.

The 1st rule in the table which matches the traffic, the parameters are enforced.

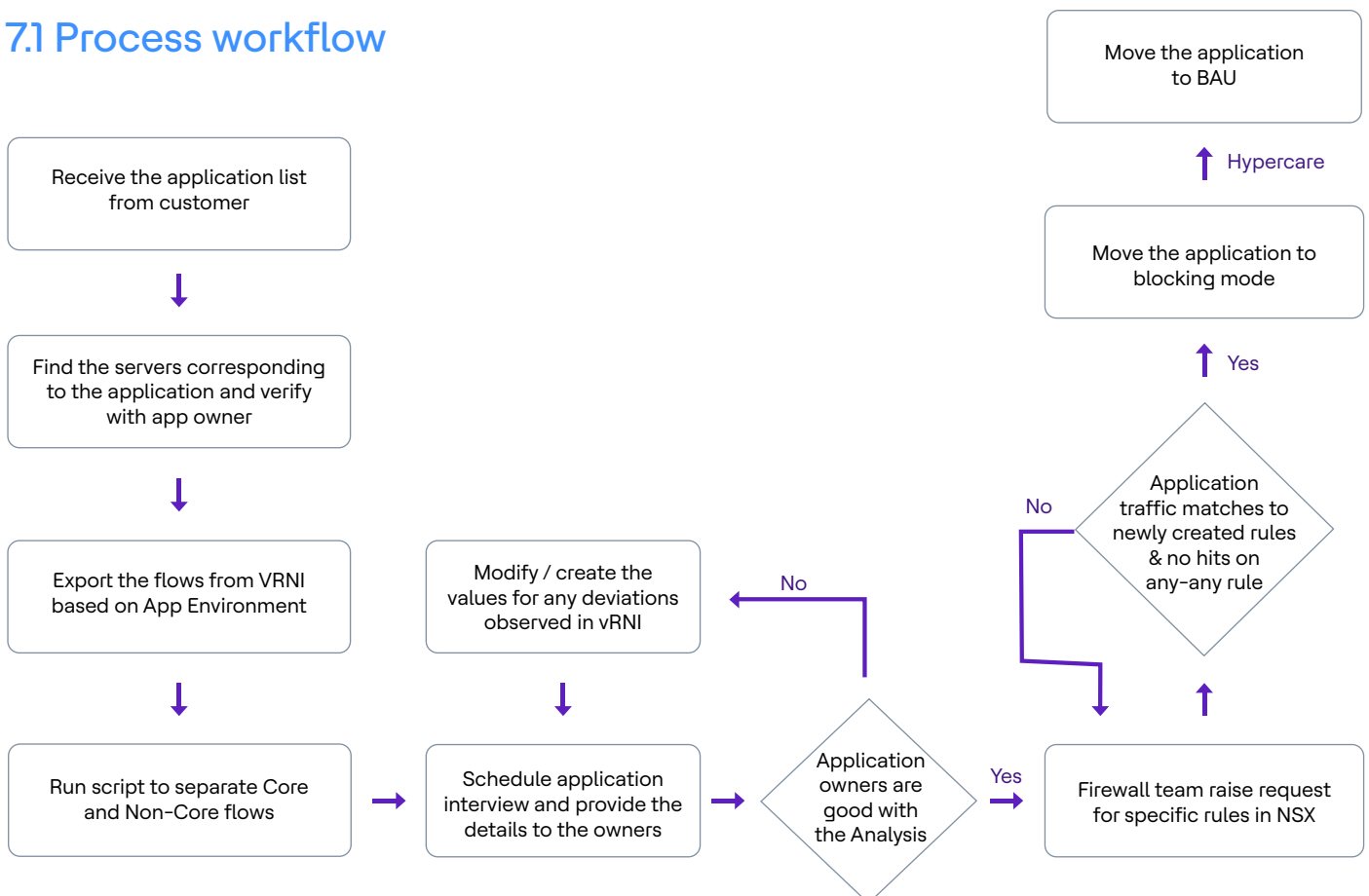
The customer is using the Infrastructure and Application category where the "infrastructure" category holds shared services (like DNS, DHCP, AD, backup, monitoring, etc) and "Application" category is holding Application environments.

7. Customer use case

HCLTech helped a customer analyze and microsegment 1000+ application environments in their new migrated environments (AVS (Azure VMware Solutions) / VCF (VMware Cloud Foundation)). We helped utilize their existing tool - vRNI (vRealize Network Insight)/ VMware Aria Operations for Networks to analyze the flows for applications and build firewall rules to secure the overall application using zero trust policy model. Along with firewall rules, HCLTech built a Flow Schematics for the security and application owners to visualize the flow for easy understanding. The application finally went through a hyper-care period of 2 weeks before moving to Business As Usual (BAU).



7.1 Process workflow



7.2 Tools used

VMware Aria
operations for
Networks / vRNI

VMware NSX-T

Service Now

Power BI

vRA / vRO

Microsoft Visio

Azure DevOps

Azure Databricks

Infoblox

7.3 Phases per application



Application analysis

Application details were gathered and checked for prerequisites like VM tagging, naming conventions.



Firewall sheet preparation and discussion

Using vRNI and Power BI, firewall sheets were prepared to discuss and finalize with application owners where they were briefed on non-secure ports and other best practices.



Rule implementation and monitoring

Created groups and implemented rules via automation and monitored the rules to see hits on any-any rule in application compartment.



Blocking

Moved any-any rule from application compartment to reject mode via approved change. This required all stakeholders to be present in the call for any urgent rules needed to ensure the proper functioning of applications.



Hypercare and BAU

The compartment was under Hypercare phase for any miss flows reported. The application was then handed over to the application owner for BAU.

7.4 Documents preparation per application

- Application compartment diagram – To visualize total number of servers and respective tiers of servers.
- Firewall sheet – All necessary groups and firewall rules.
- Flow schematics – Visualization of firewall sheet depicting all intra and inter compartment flows.
- Handover documents – All documents needed for application owner to handle it independently.



7.5 Automation tasks performed

- Pre-Checklist values check – To check segment naming, tag status and Risk and Compliance status in case the application is good to be micro-segmented.
- Scrubbing data received from vRNI using scripts – To make vRNI data easily readable by separating core and non-core applications.
- Catalog published and workflows execution using vRA / vRO
 - Firewall rule implementation – Implemented firewall rules using service now catalogue.
 - Service group / Security group creation and update – Created / updated service groups (TCP/UDP ports) and security groups (IP Address)
 - Moving the compartment to blocking phase – Modified the last rule in compartment to deny mode.
 - Policy report for the compartment – Received all firewall rules in the compartment.
- DR firewall rules replication – Replicated firewall rules in DR location based on current ruleset in Active DC.



7.6 Benefits

- Automated way of creation / modification / deletion of security and service groups and implementation of firewall rules.
- Impact limited to per application environment.
- Easier troubleshooting with fixing of the number of rules per compartment
- Added control with application owners on what flows they need to allow for end-user or other application access
- Consistent DR rules as compared to Active DC.
- Effortless review of compartment rules for audit and modification as needed.
- Auto security groups updated based on VM tagging.



7.7 Key challenges

- Shared servers across applications
- Tags missing or incorrect.
- Segment Naming convention incorrect.
- Application spread across multiple environments (AVS / VCF / On-Prem)
- Application spread across geographies.
- Multiple use cases for automation





Conclusion

Virtualization, cloud, and software-defined services have spearheaded the modernization of the data center, upending established IT models of resource provisioning and consumption. Microsegmentation enables a fundamental architectural shift, making allowlist/Zero Trust Model feasible within the modern dynamic data center. NSX micro-segmentation provides the tools and capabilities needed to build a firm foundation, securing the modern data center.

Embracing NSX-T Microsegmentation is not just a security measure; it's a strategic investment in the resilience and protection of your organization's critical assets. By implementing a well-defined microsegmentation strategy and leveraging the full potential of NSX-T, organizations can confidently navigate the complex security challenges of today's digital world.

For more information, you may write to us at HCBU-PMG@hcltech.com

HCLTech | Supercharging
Progress™

hcltech.com