NSX INTRUSION DETECTION AND PREVENTION SYSTEM
MANAGED SERVICE GUIDE FOR VMWARE CLOUD DIRECTOR

Managed VMware NSX IDS/IPS for VMware Cloud Director

For Cloud and Service Providers

Romain Decker
Cloud Infrastructure Business Group
December 2022
# Table of Contents

1. Introduction ........................................................................................................................................... 3
2. Disclaimer .................................. .......................................................................................................... 3
3. NSX Intrusion Detection & Prevention System ....................................................................................... 3
4. NSX IDS/IPS in VMware Cloud Provider Platform ............................................................................. 4
   - Deployment Considerations & Recommendations ........................................................................... 5
   - Performance Considerations & Recommendations ........................................................................ 5
5. Topology .................................................................................................................................................. 6
6. Implementation Workflow ....................................................................................................................... 7
   - Common Steps ..................................................................................................................................... 8
     - Requirements ................................................................................................................................. 8
     - Manage Signatures ....................................................................................................................... 8
     - Security Profiles .......................................................................................................................... 8
6. Distributed IDS/IPS ................................................................................................................................. 10
7. Gateway IDS/IPS ..................................................................................................................................... 15
8. Day 2 Operations .................................................................................................................................... 17
   - Monitoring IDS/IPS .......................................................................................................................... 17
   - IDS/IPS Events ............................................................................................................................... 17
9. Conclusion ............................................................................................................................................... 20
Introduction
This white paper is intended for VMware Cloud Providers who are interested in offering VMware NSX IDS/IPS in their multi-tenant environments managed by VMware Cloud Director™ (VCD).

Intrusion Detection Systems (IDS) emerged in the late 1990s to detect traffic patterns indicative of incoming attacks. In the 2000s, IDS morphed into Intrusion Prevention Systems (IPS) as it acquired additional security capabilities. Over the years, IDS/IPS has become a standard capability of the network security stack.

VMware NSX® provides Intrusion Detection and Prevention Service (IDS/IPS) to monitor east-west and north-south traffic to detect malicious traffic patterns not only by comparing the traffic against a known set of intrusion detection signatures but also by identifying anomalous behavior.

This guide will guide through the steps to enable system administrators to implement those solutions as a managed service for VMware Cloud Director users. In the proposed implementation, the components are configured and managed separately from VMware Cloud Director.

Disclaimer
This document aims to describe one option to provide managed NSX IDS/IPS for VMware Cloud Director. As such, some topics are outside the scope of this document:

- All configuration permutations and implementation steps can vary based on multiple factors, such as network and data center design, existing security policies, and topology.
- The proposed implementation depends on NSX-T 3.2.1 or later.
- The actual implementation may differ, as Cloud Director and NSX offer a wide range of possibilities on how to be implemented.

General knowledge of networking and security, as well as on VMware Cloud Director concepts, is also required.

This document is not intended to be a comprehensive installation guide, nor is it intended to replace the essential information you will find in the VMware NSX Security Admin Guide.

NSX Intrusion Detection & Prevention System
While the goal of a firewall is to limit the attack surface, by only allowing traffic on channels that need to be open for the application to function, the goal of an Intrusion Detection/Prevention system is to detect and prevent attackers from taking advantage of vulnerabilities that may exist in applications.

Over the years, IDS/IPS has become a standard capability of the network security stack. Despite the history, cost and operational complexity have restricted the use of IDS/IPS to specific network segments, such as those on an enterprises’ perimeter with public networks. With the rise of distributed applications and microservices, network traffic in the data center has increased manifold. Simultaneously, the data center boundary has become diffuse with increased connectivity of applications in the data center to the public cloud and end-user devices. Thus, IDS/IPS has become increasingly applicable to the data center as a layer of security.

VMware NSX provides a new architectural approach to IDS/IPS that changes the traditional trade-offs between cost or operational complexity, and the extent of security coverage.

VMware NSX supports IDS/IPS capability on the following firewalls:

- **Distributed Firewall** – Prior to NSX-T Data Center 3.2, implementation of IDS was limited to knowledge-based signatures. Knowledge-based signatures incorporate specific knowledge or pattern that corresponds to a known type of attack. In this approach, IDS attempts to detect intrusions based on already known malicious instruction sequences specified in signatures. Thus, knowledge-based signatures are limited to attacks that are already known and cannot cover targeted or zero-day threats. Starting with NSX-T Data Center 3.2, IDS also supports behavior-based detection. Behavior-based detection attempts to identify anomalous behavior by pinpointing interesting events that are different or unusual compared to a baseline or normal traffic.

- **Gateway Firewall** – Starting with NSX-T Data Center 3.2.1, IDS/IPS is also available on Gateway Firewall.
NSX Distributed IDS/IPS uses an all-software distributed approach that moves traffic inspection out to every workload. It eliminates the need to hair-pin traffic to discrete appliances, ensuring comprehensive coverage without any blind spots.

Figure 1 – Distributed Firewall and IDS/IPS in NSX

**NSX IDS/IPS in VMware Cloud Provider Platform**

VMware Cloud Director is a leading cloud service-delivery platform used by some of the world’s most popular cloud providers to operate and manage successful cloud-service businesses. Using VMware Cloud Director, cloud providers deliver secure, efficient, and elastic cloud resources to thousands of enterprises and IT teams across the world.

While VMware Cloud Director empowers customers to deploy workloads in secured, isolated, and multi-tenant environments, the NSX IDS/IPS capabilities cannot yet be consumed directly from the VCD portals.¹

The approach described in this document is to configure IDS/IPS profiles and rules from NSX and apply the inspection to pre-existing objects that VMware Cloud Director creates and manages (dynamic security groups and edge gateways).

Use cases for NSX Distributed IDS/IPS include:

- Easily achieving regulatory compliance
- Virtualizing security zones
- Replacing discrete appliances
- Virtually patch vulnerabilities

¹ Planned for an upcoming release of VMware Cloud Director.
Deployment Considerations & Recommendations
There are several important factors to consider ensuring a successful configuration and smooth operations:

- Although VLAN and overlay segments are supported, the proposed implementation is to apply IDS/IPS rules to routed and isolated organization VDC networks (overlay NSX-T segments).
- If Distributed Firewall is enabled, the traffic needs to be allowed by DFW to be passed through the IDS/IPS engine.
- 7.0U3c is the minimum recommended ESXi version (as it fixes a syslog log truncate bug).
- IDS/IPS is an NSX feature enforced by a license.

Performance Considerations & Recommendations
Optimizing the performance is essential to ensure that the system can handle the demands of its users and operate efficiently. In this section, we will discuss some key considerations and recommendations in that area.

The distributed IDPS engine runs in a shared memory space and uses one thread per host core and up to 5 CPU cores per host. The number of threads is determined by the number of cores on the vSphere host. In NSX-T 3.2, each IDPS engine has one thread per host core, and this cannot be modified. The memory allocated to the IDPS engine is a shared 1 gigabyte space and cannot be adjusted. DRS does not have the ability to monitor user-space, so it is not possible to instruct DRS to move workloads.

Traffic destined to the IDPS engine can exceed a given ESXi host’s capacity in either CPU or memory. By design, the default action when oversubscription happens is to silently drop the packets. Care should be taken to ensure that this is kept in mind when positioning this in a customer’s environment. The use of network monitoring tools like VRNI can be extremely useful when undertaking this planning.

Consider the following scale and performance recommendations:

- Start small: you should ideally isolate IDS/IPS service on a specific vSphere cluster (consumed as a provider VDC in VMware Cloud Director).
- Only inspect traffic that is relevant. There are several ways to influence the quantity of traffic that will be inspected: directionality of the inspection, Applied to, exclude traffic that does not need to be inspected or cannot be inspected (storage traffic, etc.). Keep in mind that there is no visibility into encrypted traffic with the Distributed IDS.
- Should gateway IDPS be considered, NSX Edge VMs with at least the Large form factor must be deployed. The Gateway does have a SSL decryption capability and it can be combined with IDS/IPS policy to inspect encrypted traffic.
- Ensure each host on which distributed IDS/IPS is enabled is not CPU constrained. Userworlds like IDS/IPS cannot reserve CPU cores, so other process like VMs have priority access to the CPU.
- It is important to consider that there is currently a per host 140K PPS limitation on the DVFilter Channel. This is per host and anything that exceeds this will result in traffic being dropped.
**Topology**

With VMware NSX, you have two options for inspecting traffic: the distributed IDS/IPS and the gateway IDS/IPS. You can choose to use one or the other, or both simultaneously, as they are not mutually exclusive.

The choice depends on the type and the architecture of applications that have to be protected, the type of protection desired (east-west vs north-south) as well as expected performance.

When used simultaneously, tenant A can for example leverage distributed IDS/IPS and tenant B gateway IDS/IPS. NSX distributed IDPS rules are applied to the entire Distributed Firewall by default, which may affect performance if not carefully managed.

VMware Cloud Director already manages several NSX objects, including a dynamic security group that contains all VMs connected to organization VDC networks scoped to that data center group. For distributed IDS/IPS, that security group will be used in the Applied To field to ensure that proper traffic inspection is only applied to relevant workloads.

![Figure 2 – VMware NSX IDS/IPS traffic inspection in VMware Cloud Director](image-url)
Implementation Workflow
This section explains steps for common configuration tasks to be performed so that system administrators can implement NSX IDS/IPS as a managed service for their VMware Cloud Director tenants. Please note that the actual implementation may differ in your environment.

Preparing the data center for NSX Intrusion Detection/Prevention involves multiple steps. The following table shows the high-level tasks required for the implementation of the solution, as well as their scope.

<table>
<thead>
<tr>
<th>TASK</th>
<th>TYPE</th>
<th>LOCATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Both</td>
<td>N/A</td>
<td>Confirm that the platform is in a healthy state before starting the implementation. Ensure proper NSX licenses are available and assigned.</td>
</tr>
<tr>
<td>Manage Signatures</td>
<td>Both</td>
<td>IDS/IPS &amp; Malware Prevention Settings tab</td>
<td>(optional) Configure an Internet Proxy Server if required. Ensure that NSX can auto-update new signature versions.</td>
</tr>
<tr>
<td>Security Profiles</td>
<td>Both</td>
<td>IDS/IPS &amp; Malware Prevention Settings tab</td>
<td>Create the required security profile(s).</td>
</tr>
</tbody>
</table>

**STEPS RELATED TO DISTRIBUTED IDPS**

<table>
<thead>
<tr>
<th>TASK</th>
<th>TYPE</th>
<th>LOCATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Group</td>
<td>Distributed IDPS</td>
<td>VMware Cloud Director Tenant Portal</td>
<td>(optional) Create a data center group if required. If distributed firewall is enabled for the concerned virtual machines and networks, ensure traffic is allowed.</td>
</tr>
<tr>
<td>Distributed IDPS Rules</td>
<td>Distributed IDPS</td>
<td>IDS/IPS &amp; Malware Prevention Distributed Rules tab</td>
<td>Add a distributed rule policy to create a section for organizing the distributed IDS/IPS rules. Add relevant rule(s) and configure appropriate sources, destinations, services and security profile fields. Set the Applied To field to the dynamic security group matching the data center group object.</td>
</tr>
</tbody>
</table>

**STEPS RELATED TO GATEWAY IDPS**

<table>
<thead>
<tr>
<th>TASK</th>
<th>TYPE</th>
<th>LOCATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Gateway</td>
<td>Gateway IDPS</td>
<td>VMware Cloud Director Tenant Portal</td>
<td>(optional) Create an edge gateway if required.</td>
</tr>
<tr>
<td>Gateway IDPS Rules</td>
<td>Gateway IDPS</td>
<td>IDS/IPS &amp; Malware Prevention Gateway Rules tab</td>
<td>Select the appropriate Tier-1 Gateway from the drop-down menu. Add a gateway rule policy to create a section for organizing the gateway IDS/IPS rules for that specific Tier-1 Gateway. Add relevant rule(s) and configure appropriate sources, destinations, services, and security profile. Validate that the Applied To field is set to the Tier-1 Gateway.</td>
</tr>
</tbody>
</table>

Table 1 – High-level implementation plan
Common Steps
This section describes the initial steps that are common to both solutions, distributed and gateway IDS/IPS.

Requirements
You can set up NSX IDS/IPS in your NSX-T Data Center environment only when using an appropriate license.

If NSX detects that appropriate licenses are not added, the following warning message will appear in the IDS/IPS & Malware Prevention configuration page: “This feature is not supported with the current applied license.”.

If you’re planning to use gateway IDS/IPS, ensure that the concerned NSX Edge VMs are deployed with at least the Large form factor.

Manage Signatures
When Internet connectivity is configured in your data center, NSX Manager checks for availability of new intrusion detection signatures on a VMware cloud-based service every 20 minutes.

Turn on the Auto Update new versions option to automatically apply intrusion detection signatures to the hosts and edges in the data center after they are downloaded from the cloud.

Note: If the data center does not have an Internet connectivity, you can manually download the IDS signature bundle (.zip) file, and then upload the file to the NSX Manager.

Click View and manage global signature set to globally change the action of specific signatures to alert, drop, or reject.

Select an Action for the signature and click Save. The changes done in global signature management settings are applicable to all IDS/IPS profiles. However, if you update the signature settings in an IDS/IPS profile, the profile settings take precedence.

Security Profiles
The key with any successful IDPS deployment is to tune the number of patterns or signatures to reflect what the workloads are running. This will limit signature evaluation to the relevant traffic on the workload. For example, WordPress and Apache signatures are irrelevant to DB workloads. This will reduce the number of false positives (noise) and will not consume needless resources on the ESXi servers themselves.

In a VMware Cloud Director context, create at least one security profile per tenant to group signatures, which can then be applied to selected distributed or gateway rules.

2. Select the required Intrusion Severities that you want to include in the profile.
3. (Optional) Filter signatures to include in the profile by Attack Types, CVSS, Attack Targets, and Products Affected.
4. To change the action on a specific signature, click Manage signatures for this profile and filter based on the CVE number to see specific signatures that are included in the profile. In the Action column, select the action you want taken: Alert, Drop or Reject.

Note: Some signatures come with a default action set to “Alert”. For the NSX Distributed IDS/IPS to drop the offending traffic in addition to alerting, you will need to change the action to either “Drop” or “Reject”.
Security profile considerations:

- You can create 25 custom profiles in addition to the default profile.
- A security profile may be attached to Distributed IDPS rules and/or Gateway IDPS rules.
- The default IDS profile includes critical severities and cannot be edited.

Distributed IDS/IPS

From the VMware Cloud Director tenant portal, ensure you have a data center group configured, even if the concerned tenant is running his workloads from a single VDC.

Data center group networks backed by NSX provide level-2 network sharing and distributed firewall (DFW) rules that are applied across a data center group. VMware Cloud Director creates and manages an NSX dynamic security group that matches all virtual machines that are connected to organization VDC networks scoped to data center group.
When you configure a distributed IDPS rule, use the "Applied-To" configuration parameter to select the security group matching the relevant data center group, to apply that rule to only the hypervisors with VMs in that group. If you don’t do this, the rule will be applied to “DFW” which is all hypervisors. This also ensures that any new or removed workloads will get the appropriate treatment by the security policy.

Another recommendation is to use directionality when you configure IDPS rules. If directionality is not configured, the traffic will be inspected in both directions, which is costly: the default setting is “In-Out” which means the traffic will be evaluated twice (one in each direction) and depending on the hypervisor, this may be a performance concern. For example, for a web server in a DMZ, you would configure inbound web requests with directionality “In” as that traffic should be exclusively inbound. Directionality is configured per IDPS rule.

---

**Figure 5** – VMware Cloud Director Data Center Group for the ACME Tenant

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Type</th>
<th>Network Provider Type</th>
<th>Participating VDCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>acme-dcgroup</td>
<td>Normal</td>
<td>Local</td>
<td>NSX-T</td>
<td>2</td>
</tr>
</tbody>
</table>

---

*VMware Cloud Director*
Enable NSX data center for distributed IDS/IPS:

6. In the Activate Hosts & Clusters for East-West Traffic section, select the ESXi host clusters where you want to turn on NSX IDS/IPS on the east-west traffic. Note that the activation is instantaneous as the kernel module is already installed.

![Figure 6 - Activate vSphere Cluster(s) for East-West Traffic](image)

Create distributed IDPS rules to associate the traffic patterns to inspect with previously created security profiles:

2. Create a new Policy (section to organize rules).
3. Add one or multiple Rules (depending on the traffic patterns to inspect).
   a. Adapt the Sources, Destinations and Services columns based on the traffic that requires IDS/IPS inspection.
   b. Select the Security Profile previously created.
c. In the Applied To field, select the dynamic security groups that has the same name as the data center group in VMware Cloud Director.

d. Select the appropriate mode (see below).

e. (optional) Click the gear icon to configure other rule setting: logging, log label, IP protocol and direction.

4. Click Publish.

Figure 7 - Distributed IDS/IPS Rules Creation

Please note that the sources, destinations, and services field are left to their default (Any) in the above screenshot. This is done to avoid any confusion, but those fields should be configured accordingly in a production environment.
Figure 8 – Applied To Field set to the Dynamic Security Group matching the Data Center Group

Regarding the mode:

- **Detect Only** – The rule detects intrusions against signatures and does not take any action.
- **Detect & Prevent** – The rule detects intrusions against signatures and either drops or rejects the traffic depending on the signature configuration in the IDS/IPS profile or in the global signature configuration.

Figure 9 – Detection or Detection and Prevention Mode

A best practice is to start with Detect Only mode and move to Detect & Prevent after initial deployment and tuning.
Gateway IDS/IPS
In NSX-T Data Center 3.2.0, NSX IDS/IPS on Gateway Firewall was available in tech preview mode only. Starting with NSX-T Data Center 3.2.1, this feature is available for production environments and has full support.

An NSX edge gateway provides a routed organization VDC network or a data center group network with connectivity to external networks and IP management properties. It can also provide services such as firewall, network address translation (NAT), IPSec VPN, DNS forwarding, and DHCP, which is enabled by default.

From the VMware Cloud Director tenant portal, ensure you have an NSX edge gateway configured. VMware Cloud Director creates and manages a Tier-1 Gateway that matches the NSX edge gateway object.

When you configure a gateway IDPS rule, set the “Applied-To” field to match the appropriate Tier-1 Gateway. This ensures that workloads connected to that gateway will get the appropriate treatment by the security policy.

The gateway IDS/IPS capability must be enabled for specific Tier-1 Gateways:

2. In the Activate Gateways for North-South Traffic section, select the gateway(s) where you want to turn on NSX IDS/IPS on the north-south traffic.

Figure 10 – Activate Gateways for North-South Traffic
Create gateway IDPS rules to associate the traffic patterns to inspect with previously created security profiles:

2. Select the relevant gateway from the drop-down menu.
3. Create a new Policy (section to organize rules).
4. Add one or multiple Rules (depending on the traffic patterns to inspect).
   a. Adapt the Sources, Destinations and Services columns based on the traffic that requires IDS/IPS inspection.
   b. Select the Security Profile previously created.
   c. In the Applied To field, validate that the gateway is already selected.
   d. Select the appropriate mode.
   e. (optional) Click the gear icon to configure other rule setting: logging, log label, IP protocol and direction.
5. Click Publish.

Figure 11 – Gateway IDS/IPS Rules Creation

Please note that the sources, destinations, and services field are left to their default (Any) in the above screenshot. This is done to avoid any confusion, but those fields should be configured accordingly in a production environment.
Day 2 Operations

Monitoring IDS/IPS
Successful implementation of any IDPS system requires some proper instrumentation and day-2 operations. The NSX-T content Pack for VMware Aria Operations for Logs (formerly vRealize Log Insight, a.k.a. vRLI) can help show a unified dashboard of events.

VMware Aria Operations for Networks (formerly vRealize Network Insight, a.k.a. vRNI) can also be a tool to support day-2 operations of the IDPS. Watching for increases in traffic flows or other trends in things like host CPU and Memory utilization will help avoid any issues from becoming more serious.

IDS/IPS Events
You can monitor events and view data of the last 14 days. To view intrusion events, navigate to Security > IDS/IPS. You can filter the events based on multiple criteria: attack target, attack type, CVSS, VM Name, etc.

![IDS/IPS Events Dashboard](image)

Figure 12 – IDS/IPS Events Dashboard
Click the arrow next to an event to view details.

Figure 13 – IDS/IPS Event Details

You can click on the number in the Workloads column to discover which VMs are affected.

Figure 14 – Affected Workload Details

NSX-T components write logs locally to the ESXi hosts themselves and can forward the IDS events to a centralized SYSLOG server. Logging to a Security Information and Event Management (SIEM) is an option to retrieve the event a central log repository. Events are sent in the EVE.JSON format for which many SIEMs have pre-existing parsers/dashboards. To send all NSX-T Data Center IDS/IPS logs to a central log repository:

1. Ensure that the NSX-T manager and ESXi hosts are setup to forward syslog messages to the central log repository.
2. Set the variable `global__idsevents__to__syslog.enabled` to true.
This last step can only be achieved using API.

1. Run the below API GET call to NSX Manager to retrieve the current syslog configuration. Note the Revision number from the API return body.
   a. URI: https://<nsxt-fqdn-or-IP>/api/v1/global-configs/IdsGlobalConfig

2. Now run a PUT call to enable syslog.
   a. URI: https://<nsxt-fqdn-or-IP>/api/v1/global-configs/IdsGlobalConfig
   b. Body:
      ```
      {
        "global_ids_events_to_syslog_enabled": true,
        "resource_type": "IdsGlobalConfig",
        "_revision": 36 (change this to the revision number from the get call)
      }
      ```

Once the logs are collected by a SIEM, you can filter on IDS/IPS events using the string **IDS_EVT**.

![IDS_EVT](image)

Figure 15 – IDS/IPS Events Filtering in vRealize Log Insight
Conclusion

The purpose of this white paper is to provide guidance to VMware Cloud Providers on how to offer VMware NSX IDS/IPS in their multi-tenant environments managed by VMware Cloud Director (VCD).

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are security capabilities that monitor traffic patterns to detect and prevent incoming attacks. VMware NSX provides IDS/IPS service to monitor east-west and north-south traffic and detect malicious activity by comparing traffic against known intrusion detection signatures and identifying anomalous behavior.