

# VSX – Migrate One Virtual System (VS) at a time to a new appliance

Joseph Audet / Michael Lefebvre  
Security Engineer

June 30, 2019

## Table of Contents:

- What is VSX?
- Use Case - Why migrate one Virtual System at a time?
- Migration Scenario - Architecture
- Backing up all data (Central & Local configurations)
- Migration Process Overview
- Reference Articles

## **DISCLAIMERS:**

This document assumes experience with the VSX product, and intermediate to advanced knowledge of the various components and will not cover them from a tutorial perspective. It is intended to demonstrate how to solve a specific scenario. Work with your account team and/or TAC for all migration planning to ensure a safe, supported migration.

This document does NOT cover licensing. Work with your account manager / security engineer to ensure you have proper licensing for any extra virtual systems that may be needed for the staging period.

## What is VSX?

Check Point's Virtual Systems technology has been providing value and protection for enterprises and service providers. This proven technology enables organizations to consolidate up to 250 gateways into a hardware platform providing savings on both capital equipment investments and ongoing support and maintenance. The streamlined management of the virtualized gateways further improves the operational efficiency of a resource-challenged IT department, bringing the needed simplicity to network security.

For more information please see the official product page:

<https://www.checkpoint.com/products/virtual-systems/>

## Use Case - Why migrate one Virtual System at a time?

Customer presented the following scenario:

Environment overview:

- 22 Virtual Systems
- R80.20 MDS server with (1) Domain / CMA per Virtual System
- 249 sub interfaces across the 22 VS's
- Thousands of effected devices that pass traffic through the appliances
- Virtual Router based architecture
- R77.30 appliance code

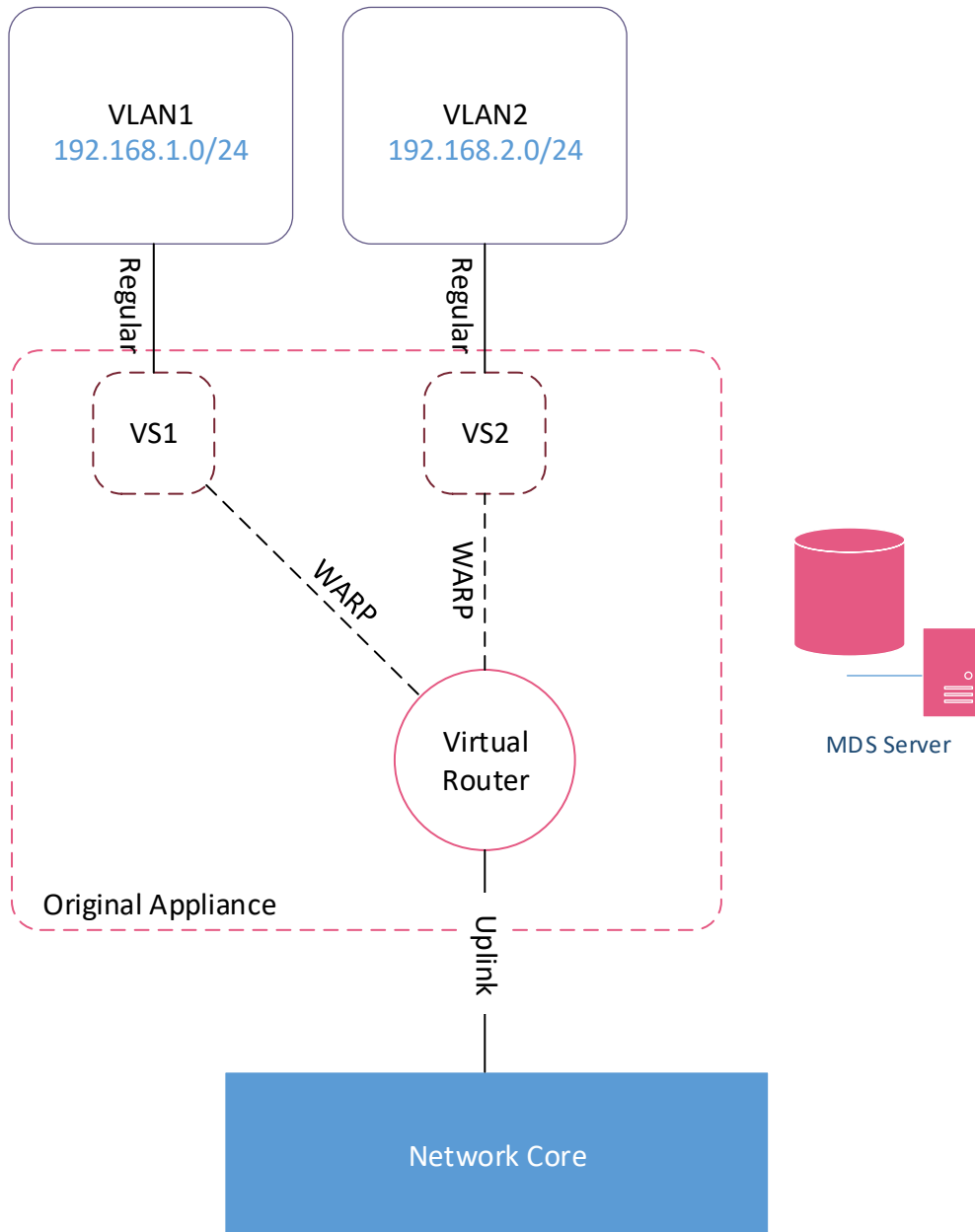
Customer wanted to make the following changes to their environment:

- Upgrade hardware
- Upgrade to R80.20
- Change from Virtual Router (VR) to Virtual Switch (VSW) leveraging Virtual System Load Sharing (VSLS)

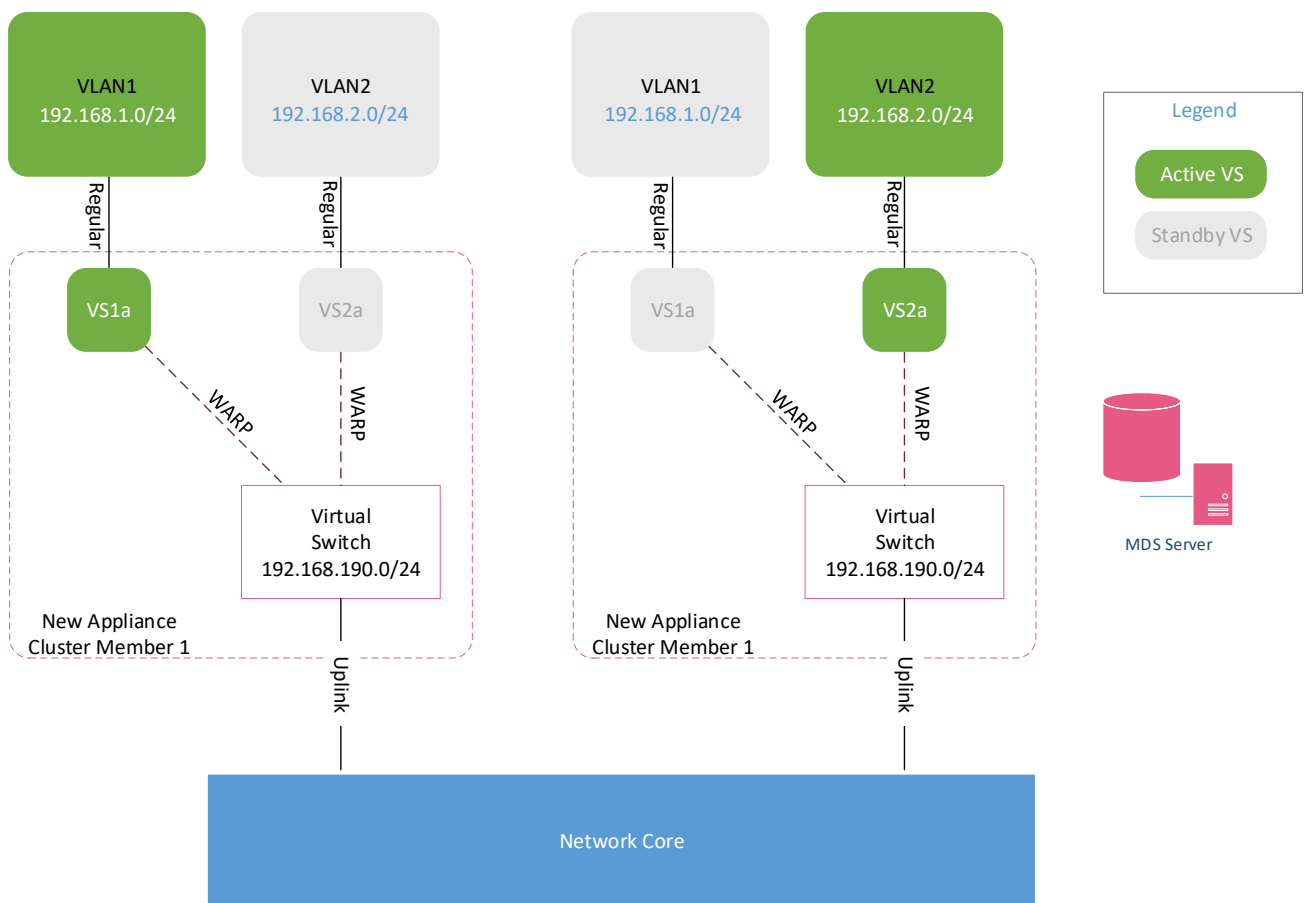
The objectives the customer desired made it extremely difficult to do an entire appliance swap at one time. A process was designed, and tested in a lab that allowed for minimal downtime, the ability to revert quickly, and achieve their objectives in a controlled manner.

## Migration Scenario – Architecture

Original configuration (cluster not depicted visually):



Desired end state:



Using VSLS the customer would be able to spread the load across (2) or more appliances by having some VS's be active on one piece of hardware, and the rest active on another piece of hardware achieving an Active/Active setup.

## Backing up all data (Central & Local configurations)

VSX configuration data is stored in 2 places:

- Central – VS build, interface info, static routes, blades, policy
- Local – Interface bonding, DHCP relay, dynamic routing, kernel modifications

Backing up the management server is not enough for a disaster recovery of the appliances. You also need to backup any local appliance specific configuration data. This information is also used to replicate the settings for a migration.

Backup the management server following Check Point recommended best practices for the management server. In this case we took an MDS backup and exported it to a new server, as well as an appliance snapshot.

To back up the local appliance specific information, refer to the following SK:

### How to backup and restore VSX gateway

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolution\\_details=&solutionid=sk100395](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolution_details=&solutionid=sk100395)

You can do these steps manually, however Niels Van Sluis wrote a script that does all of the steps in the SK and packages everything up in a nice neat TAR file:

CheckMates Article:

<https://community.checkpoint.com/t5/General-Management-Topics/Show-configuration-scripts-VSX/td-p/21770>

Direct GitHub link:

<https://github.com/nvansluis/checkpoint-vsx-save-configuration>

## Migration Process Overview

The following steps will be taken to migrate the VS from the original appliance to the new appliance and allow for a quick rollback:

Prep work:

- Build, patch, cable and configure the new appliances as a VSLS cluster
- Create the new VS (either using Smart Console, or the `vsx_provisioning_tool`)
- Using the `vsx_provisioning_tool` grab a copy of the current state of the Virtual Device(s) from the management server
- Create transaction scripts for use with the `vsx_provisioning_tool` for the following:
  - Remove route propagation for all interfaces & static routes on the original VS
  - Create the same interfaces and static routes on the new VS
  - Undo all changes on both the old and new VS

Migration Steps:

**//Login to the gateway(s), disable the VS processes:**

```
cd $FWDIR/scripts/  
./vs_stop 2
```

**//Login to the management server and execute the script to disable route propagation, and  
//remove all static routes:**

```
vsx_provisioning_tool -s 192.168.1.175 -u <user> -f /home/<user>/decommission_vs1.txt
```

**// decommission\_vs1.txt – contents:**

```
transaction begin  
set interface vd vs1 name eth1.1 propagate false  
remove route vd vs1 destination 10.1.1.0/24  
transaction end
```

**//Verify unable to connect to the interface of the VS1**

**//Verify the configuration of VS1 (only the warp interface / default GW should exist):**

```
vsx_provisioning_tool -s 192.168.1.175 -u <user> -o show vd name vs1
```

**//On the management server execute the script to add the interfaces to the new VS (VS1a):**

```
vsx_provisioning_tool -s 192.168.1.175 -u <user> -f /home/<user>/provision_vs1a.txt
```

**// provision\_vs1a.txt – contents:**

```
transaction begin
add interface vd vs1a name eth1.1 ip 192.168.1.1/24 propagate true
add route vd vs1a destination 10.1.1.0/24 next_hop 192.168.1.250 propagate true
add route destination default next_hop 192.168.190.1
transaction end
```

**//Verify the configuration of VS1a**

```
vsx_provisioning_tool -s 192.168.1.175 -u <user> -o show vd name vs1a
```

**//Verify you can reach the interface on VS1a, and the network defined via a static route**

**//Perform all post checkout change testing**

**//Once all testing is complete and verified, delete the original VS1**

**Should one of the old appliances reboot, VS1 will turn back on automatically. Do NOT leave it active past the change window once testing is complete.**



## Reference Articles:

VSX Admin Guide (R80.30):

[https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP\\_R80.30\\_VSX\\_AdminGuide/html\\_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP\\_R80.30\\_VSX\\_AdminGuide/204002](https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_VSX_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_VSX_AdminGuide/204002)