Contents

Introduction

This document describes how to use the CLI in order to upgrade the software image on a Cisco ASA 5500 Series Adaptive Security Appliances failover pair.

Note: Adaptive Security Device Manager (ASDM) does not work if you upgrade (or downgrade) the security appliance software from 7.0 to 7.2 directly or upgrade (or downgrade) the ASDM software from 5.0 to 5.2 directly. You must upgrade (or downgrade) in incremental order.

For more information on how to upgrade the ASDM and the software image on ASA, refer to PIX/ASA: Upgrade a Software Image using ASDM or CLI Configuration Example

Note: In multicontext mode, you cannot use the **copy tftp flash** command to upgrade or downgrade the PIX/ASA image in all contexts; it is supported only in the System Exec mode.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance (ASA) with version 7.0 and later
- Cisco ASDM version 5.0 and later

Note: Refer to Allowing HTTPS Access for ASDM for information on how to allow the ASA to be configured by the ASDM.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco PIX 500 Series Security Appliance Software Version 7.0 and later.

Conventions

Refer to the Cisco Technical Tips Conventions for information on document conventions.

Configuration

Perform Zero-Downtime Upgrades for Failover Pairs

The two units in a failover configuration should have the same major (first number) and minor (second number) software version. However, you do not need to maintain version parity on the units during the upgrade process; you can have different versions on the software running on each unit and still maintain failover support. In order to ensure long-term compatibility and stability, Cisco recommends that you upgrade both units to the same version as soon as possible.

There are 3 types of upgrades available. They are as follows:

1. **Maintenance Release**—You can upgrade from any maintenance release to any other maintenance release within a minor release. For example, you can upgrade from 7.0(1) to 7.0(4) without first installing the maintenance releases in between.
2. **Minor Release**—You can upgrade from a minor release to the next minor release. You cannot skip a minor release. For example, you can upgrade from 7.0 to 7.1. Upgrading from 7.0 directly to 7.2 is not supported for zero-downtime upgrades; you must first upgrade to 7.1
3. **Major Release**—You can upgrade from the last minor release of the previous version to the next major release. For example, you can upgrade from 7.9 to 8.0, assuming that 7.9 is the last minor version in the 7.x release.

Upgrade an Active/Standby Failover Configuration

Complete these steps in order to upgrade two units in an *Active/Standby failover* configuration:

1. Download the new software to both units, and specify the new image to load with the boot system command.Refer to Upgrade a Software Image and ASDM Image using CLI for more information.
2. Reload the standby unit to boot the new image by entering the **failover reload-standby** command on the active unit as shown below:`active#`**`failover reload-standby`**
3. When the standby unit has finished reloading and is in the Standby Ready state, force the

active unit to fail over to the standby unit by entering the **no failover active** command on the active unit.`active#no failover active`
Note: Use the **show failover** command in order to verify that the standby unit is in the Standby Ready state.
4. Reload the former active unit (now the new standby unit) by entering the **reload** command:`newstandby#reload`
5. When the new standby unit has finished reloading and is in the Standby Ready state, return the original active unit to active status by entering the **failover active** command:`newstandby#failover active`

This completes the process of upgrading an Active/Standby Failover pair.

Upgrade an Active/Active Failover Configuration

Complete these steps in order to upgrade two units in an *Active/Active failover* configuration:

1. Download the new software to both units, and specify the new image to load with the boot system command.Refer to Upgrade a Software Image and ASDM Image using CLI for more information.
2. Make both failover groups active on the primary unit by entering the **failover active** command in the system execution space of the primary unit:`primary#failover active`
3. Reload the secondary unit to boot the new image by entering the **failover reload-standby** command in the system execution space of the primary unit:`primary#failover reload-standby`
4. When the secondary unit has finished reloading, and both failover groups are in the Standby Ready state on that unit, make both failover groups active on the secondary unit using the **no failover active** command in the system execution space of the primary unit:`primary#no failover active`
Note: Use the **show failover** command in order to verify that both failover groups are in the Standby Ready state on the secondary unit.
5. Make sure both failover groups are in the Standby Ready state on the primary unit, and then reload the primary unit using the **reload** command:`primary#reload`
6. If the failover groups are configured with the **preempt** command, they will automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with the **preempt** command, you can return them to active status on their designated units using the **failover active group** command.

Troubleshoot

%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit (or) %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit

Problem

One of these error messages appear when you try to upgrade the Cisco Adaptive Security Appliance (ASA):

```
%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit.
```

```
%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
```

Solution

These error messages are informative errors. The messages do not impact functionality of the ASA or the VPN.

These messages appear when the VPN failover subsystem cannot update IPsec-related runtime data because the corresponding IPsec tunnel has been deleted on the standby unit. In order to resolve these, run the **wr standby** command on the active unit.

Two bugs have been filed to address this behavior; you can upgrade to a software version of ASA where these bugs are fixed. Refer to Cisco bug IDs CSCtj58420 (registered customers only) and CSCtn56517 (registered customers only) for more information.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco Adaptive Security Device Manager**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**