Guide

Migrating from Cisco ASA 5500 Series to ASA 5500-X Series Midrange Appliances

Cisco ASA 5500-X Series midrange security appliances deliver next-generation security services. The ASA 5500-X Series hardware architecture was redesigned to address higher performance requirements and increase flexibility when adding new services while maintaining the compact 1-RU form factor. Customers migrating from ASA 5500 Series platforms need to consider these changes at the time of migration to the newer hardware. This document describes the best practices to follow while migrating to the new ASA 5500-X Series midrange appliances.

The Cisco ASA 5500 Series midrange appliance portfolio comprises four security appliances (ASA 5510, ASA 5520, ASA 5540, and ASA 5550). In March 2012, Cisco added five new midrange appliances to the ASA family. The new appliances carry the '-X' suffix to distinguish them and are named as follows:

- ASA 5512-X
- ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

The Cisco ASA 5500-X Series is designed to support next-generation security services while meeting the higher performance requirements of todays's networks. It is based on a multicore, 64-bit architecture and uses separate dedicated multicore chipsets for crypto and pattern matching operations. Hardware and software changes have been introduced without sacrificing the compact form factor.

Cisco ASA 5500-X Series Hardware Migration Path

The Cisco ASA 5500 Series portfolio comprises four platforms that are based on a single-CPU, 32-bit architecture. Due to architectural limitations, they are not capable of supporting next-generation security services. Table 1 lists the suggested hardware migration path to the ASA 5500-X Series. Suggested sizing approach is a conservative estimate.

Table 1. Hardware Migration Path from ASA 5500 Series to ASA 5500-X Series

ASA 5500 Series Appliance	Equivalent ASA 5500-X Series Appliance
ASA 5510	ASA 5512-X
ASA 5510 with SecPlus License	ASA 5515-X or ASA 5512-X with SecPlus License
ASA 5520	ASA 5525-X
ASA 5540	ASA 5545-X
ASA 5550	ASA 5555-X

Cisco ASA 5500-X Series Software Migration Path

Software support for the Cisco ASA 5500-X Series is available in ASA Software Release 8.6 and later. Earlier ASA Software releases will fail to load on the new appliances.

Planning for a Successful Migration

To ease the migration process, the following pre-migration checks should be performed to meet the minimum hardware and software requirements.

- Licenses do not migrate automatically. All required licenses should be acquired and applied to the new appliance before starting the migration process.
- ASA 5500-X Series appliances require ASA Software Release 8.6 or later. They do not support earlier software versions. The new appliance should be loaded with the latest ASA Software release available on Cisco.com.
- For information on upgrading the version of cisco security Manager, please visit this page.
- Upgrade ASA Software on existing 5500 Series appliances to ASA Software Release 8.4. With this upgrade, configuration will be updated to reflect licensing, NAT, and real IP address migration of ACL enhancements introduced in ASA Software Release 8.3.If ASA 5500 is running a pre 8.4 release, the preferred way is to upgrade iteratively over major revisions e.g., if the appliance is running ASA Software Release 7.2, then do following transitions: 7.2 to 7.4 to 8.0 to 8.2 to 8.4. With this approach, deprecated features are taken care of automatically during upgrades.
- Back up the configuration from the existing ASA 5500 Series appliance on a remote machine. This can be done using the CLI ‘copy’ command or using Cisco Adaptive Security Device Manager (ASDM).
- If the IPS Security Services Module (SSM) is present, back up the IPS configuration using IDM/IME or the CLI.
- During configuration backup, make sure to export certificates and keys from the old platform for reuse.

Feature License Migration

Cisco ASA feature licenses are linked to the hardware serial number. License information is not included in the configuration; as a result, licenses do not migrate when a configuration is moved from an older appliance to a newer one. All requisite licenses currently in use on an older ASA 5500 Series appliance should be acquired for the new ASA 5500-X Series appliance before proceeding with the migration process.

Cisco ASA Software Requirements for Migration

All new midrange ASA 5500-X Series appliances require ASA Software Release 8.6 or later (Table 2). Earlier versions are unsupported and will not load on the new platforms.

Table 2. Minimum Software Requirements for Migration from ASA 5500 to ASA 5500-X Appliances

ASA Appliance	Minimum Software Version	Notes
ASA 5500 Series (5510, 5520, 5540, and 5550)	ASA Software Release 8.4.2	Release 8.6 is not supported on these platforms.
ASA 5500-X Series (5512-X, 5515-X, 5525-X, 5545-X, and 5555-X)	ASA Software Release 8.6	

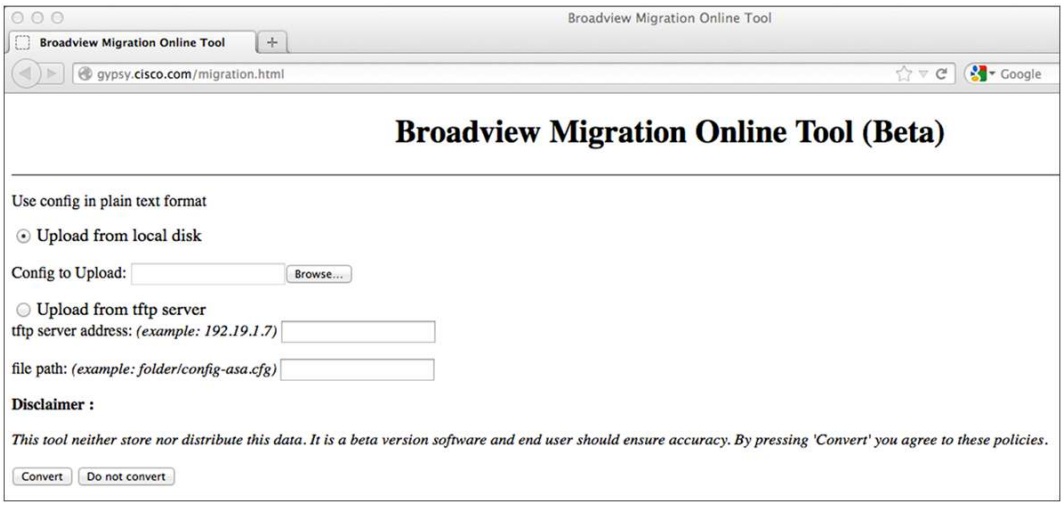
ASA 5500 Series appliances should be upgraded to ASA Software Release 8.4.2 before attempting migration to the ASA 5500-X Series. Upgrade steps are explained in detail at http://www.cisco.com/en/US/docs/security/asa/asa83/upgrading/migrating.html.

Offline upgrade of ASA 5500 Series appliances to ASA Software Release 8.4 is possible using an internal migration tool hosted at http://gypsy.cisco.com/migration.html. More information on this tool is provided in the next section.

Web-Based NAT Migration Tool for ASA 5500 Series Appliances

Cisco offers a web-based migration tool at http://gypsy.cisco.com/migration.html as an alternative option for upgrading pre-Release 8.3 ASA Software configurations to ASA Software Release 8.4 (Figure 1). Please leverage TAC or your account team for access to this internal migration tool.

Web-Based ASA Software Migration Tool



The existing configuration can be uploaded from the local machine or from a remote TFTP server located on Cisco corporate intranet. The converted configuration and the migration log are displayed in the final step. Examine the migration log carefully to identify any warnings or errors encountered during the migration process. The migrated configuration can be copied from the web tool and saved into a file.

The web migration tool is designed to address the most common scenarios seen during the migration process. The following caveats apply while using this migration tool.

- The web migration tool does not create an output configuration file. Migrated output is displayed within the webpage and should be manually saved (copy/paste) into a file for later use.
- The tool is not designed to migrate multimode configurations. It can be used only for single routed and transparent mode configurations.
- The tool has not been tested with large configuration files (files greater than 5 MB).
- The tool cannot be used to migrate configurations that contain a significant amount of nested objects and object groups in use within NAT statements and ACLs.

Figures 2 and 3 show examples of post-migration output from the web-based tool.

Figure 1. Web-Based ASA Software Migration Tool Log Output

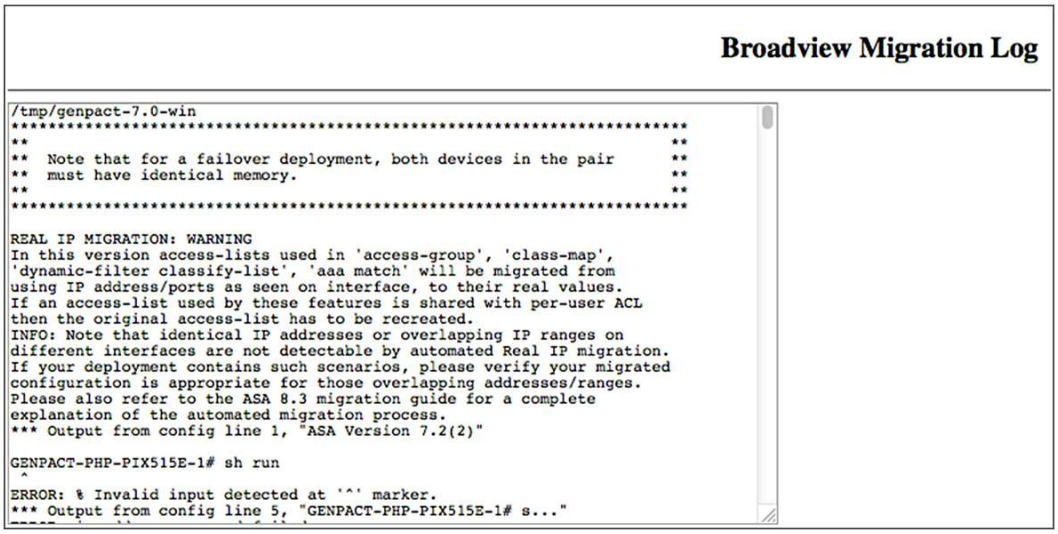
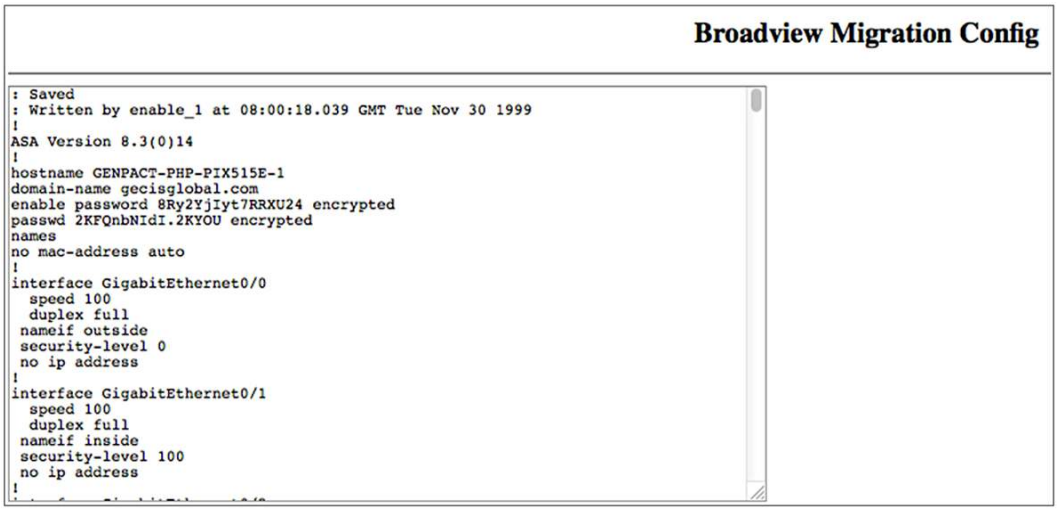


Figure 2. Web-Based ASA Software Migration Tool Configuration Output



Pre-Migration Checks on ASA 5500-X Platform

The new ASA 5500-X Series uses a different hardware architecture than the ASA 5500 Series. From an external point of view, changes can been seen in the following areas:

- A single physical management port for managing ASA and add-on security services such as IPS.
- Higher I/O density on the base platform and gigabit I/O ports only.
- No SSM option - services run on the main platform itself.

With these architectural changes, the ASA 5500 Series configuration file requires manual modifications for proper migration. The following sections outline best practices for manually editing the configuration file.

I/O Port Configuration Changes

All ASA 5500 Series appliances (except the ASA 5510 w/o SecPlus license) have gigabit ports. The change suggested below applies only to migrations from the ASA 5510. While migrating the configuration file, all interface names (including sub-interfaces) should be edited to reflect the gigabit ports present on the ASA 5500-X appliance.

Here is an example of how to edit interfaces for a 5510 configuration that is being migrated to a 5515-X appliance.

ASA 5510 Configuration

```
! Physical Interface
  interface Ethernet0/1
  no nameif
  no security-level
  no ip address
  no shutdown
! Creating Subinterfaces on interface E0/1 (two logical networks)
  interface Ethernet0/1.120
  vlan 1222
  nameif fw-out
  security-level 50
  ip address 172.16.61.1 255.255.255.0
```

Modified ASA 5515-X Configuration

```
! Physical Interface
  interface GigabitEthernet0/1
  no nameif
  no security-level
  no ip address
  no shutdown
! Creating Subinterfaces on interface G0/1 (two logical networks)
  interface GigabitEthernet0/1.1201
  vlan 1222
  nameif fw-out
  security-level 50
  ip address 172.16.61.1 255.255.255.0
```

Management Port Configuration Changes

The ASA 5500-X Series introduced a shared management port for firewall and IPS services.,There are certain caveats to follow during migration from the ASA 5500 Series.

- The shared management port cannot be used as a data port. All through-the-box traffic arriving at the management port will be dropped implicitly. This cannot be disabled.
- The shared management port cannot be used as a part of a high availability configuration.

If the ASA management port (M0/0) on the ASA 5500 Series appliance was being used as a data port, the configuration associated with that port should be moved to one of the gigabit data ports numbered above G0/3.

Here is a sample configuration for an ASA 5520 to ASA 5525-X migration.

ASA 5520 Configuration

```
! Dedicated Management Interface
  interface Management0/0
  no nameif
  no security-level
  no ip address
  no management-only
  no shutdown !

! Subinterfaces on interface M0/0
  interface Management0/0.120
  vlan 1222
  nameif fw-out
  security-level 50
  ip address 172.16.61.1 255.255.255.0
```

ASA 5515-X Configuration

```
! Dedicated Management Interface
  interface Management0/0
  no nameif
  no security-level
  no ip address
  management-only
  no shutdown

! Management Interface Migrated to GigabitEthernet0/3
  interface GigabitEthernet0/3
  no nameif
  no security-level
  no ip address
  no shutdown

! Subinterfaces on interface G0/3
```

```
interface GigabitEthernet0/3.1201
vlan 1222
nameif fw-out
security-level 50
ip address 172.16.61.1 255.255.255.0
```

Since GigabitEthernet0/3 interface and above do not exist on the ASA 5500 Series, there should be no configuration conflict with the above migration. Similarly, if the management interface was in use for failover configuration, it should be migrated to one of the newer unused interfaces on the ASA 5500-X appliance.

The following configuration changes apply when migrating ASA and IPS services from ASA 5500 Series appliances. Dedicated management ports were used for ASA and IPS services on the ASA 5500 Series. On ASA 5500-X Series appliances, firewall and IPS management share a single management port. With this architectural change, multiple deployment options are possible when using the shared management port. Deployment options are explained at: http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_tech_note09186a0080bd5d03.shtml.

A careful review of the above document is required before implementing the correct deployment option and configuration changes on the new appliance.

IPS Configuration Migration

IPS configuration file migration does not require any manual changes. Management port changes should be carefully checked before migrating the IPS service. Licensing caveats mentioned for ASA appliances also apply to the IPS service. Enabling IPS service is a two-step process that requires license enablement on the ASA appliance and within the IPS service. These steps are documented on the following techzone article. https://techzone.cisco.com/t5/Intrusion-Preventions-Systems/Troubleshooting-common-ASA-55x5-IPS-K9-Saleen-issues/ta-p/32627.

Summary

Migrating from the ASA 5500 Series to the new ASA 5500-X Series is a multistep process that requires a combination of migration tools and manual changes. This document provides a step-by-step approach designed to ease the migration process and avoid major disruption of network services.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-727453-01 05/13