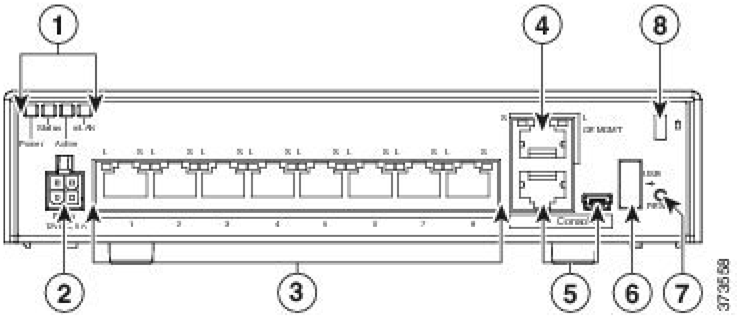
Cisco ASA 5506-X Compatibility

Last updated December 6, 2017

Cisco System has announced the end of the life for Cisco ASA 5505 Adaptive Security Appliance. To replace this appliance in the CCNA Security equipment bundle, Cisco ASA 5506-X series using asa981-lfbff-k8.SPA with ASDM asdm-781.bin was tested for its compatibility in CCNA Security version 2.0 curriculum.

The ASA 5506-X can support the current CCNA Security curriculum with some caveats. The naming conventions for Ethernet ports on the ASA 5506-X are different from those identified in the current curricula lab instructions. Furthermore, the VLAN commands associated with the network data ports are no longer necessary because the ASA 5506-X network data ports, the G1/1 - G1/8 are Layer 3 ports. The ASA-5506X has a management port that is not used in the CCNA Security 2.0 curriculum. The illustration below displays the rear panel of the ASA 5506-X.



Number	Description
1	Status LEDs
2	Power cord socket
3	Network data ports
4	Management port
5	Console ports
6	USB port
7	Reset button
8	Lock slot

For the ASA 5506-X, the G1/1 port is attached to the cable that is connected to the Ethernet port of the WAN device. The G1/2 port is connected to the cable that is connected to the Ethernet port associated with the internal devices. Furthermore, the DHCP pool is no longer limited to 32 addresses. If the user credentials created with ASDM fails to log in, the user credentials created with CLI can be used to log in instead. Furthermore, SSH access requires an RSA key for a successful connection. An RSA key can be generated within ASDM if the RSA key created in CLI fails to establish a connection.

There are several hardware features and commands that are either no longer available or differ from the curricula lab instructions. The table below lists the commands that are affected when ASA 5506-X is used to perform the labs in the current CCNA Security curriculum.

Summary of Changes

Hardware / Commands	Cisco ASA 5506-X
GigabitEthernet 1/1	outside interface, DHCP from modem
GigabitEthernet 1/2	inside interface, ASA Management Gateway
Management 1/1	ASA FirePower Management
DHCP pool	No longer restricted to 32 addresses
User credentials	Use the user credentials created with CLI if the user credentials created with ASDM fails to log in.
SSH access	For SSH access to be successful, an RSA key is needed. To generate an RSA key for SSH access in ASDM, click **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**. Select **Identify Certificates** > **Add**. Select **Add a new identity certificate**. Click **New**. Verify RSA is selected and use Use default key pair name and click **Generate Now**. Click **Cancel** > **Cancel** to return to Identify Certificate.
VLAN associations	No longer necessary