ASA 8.x: Cisco ASA in Multiple Context Mode Synchronized with NTP Server Configuration Example

Contents

Introduction

This document provides a sample configuration of how to synchronize the clock of the Cisco Adaptive Security Appliance (ASA) in multiple context mode with that of a Network Time Protocol (NTP) server.

NTP is a protocol used in order to synchronize the clocks of different network entities. It uses UDP/123. The primary reason to use this protocol is to avoid the effects of variable latency over the data networks.

In this scenario, Cisco ASA is in multiple context mode. Admin and Test1 are the two different contexts. In order to configure the Cisco ASA as an NTP client, you need to specify the **NTP Server** command in the system execution space only because this command does not support the context 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 ASA with Software Release Version 8.2 and later
- Cisco Adaptive Security Device Manager (ASDM) with Software Release version 6.3 and later

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.

Conventions

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

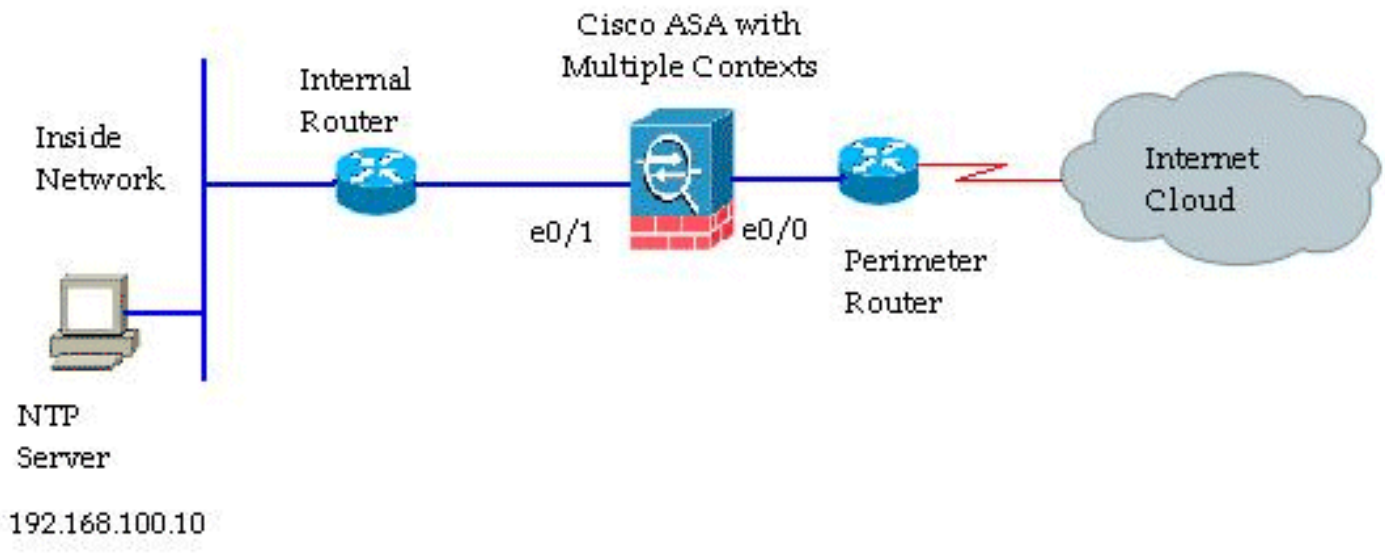
Configure

In this section, you are presented with the information needed in order to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

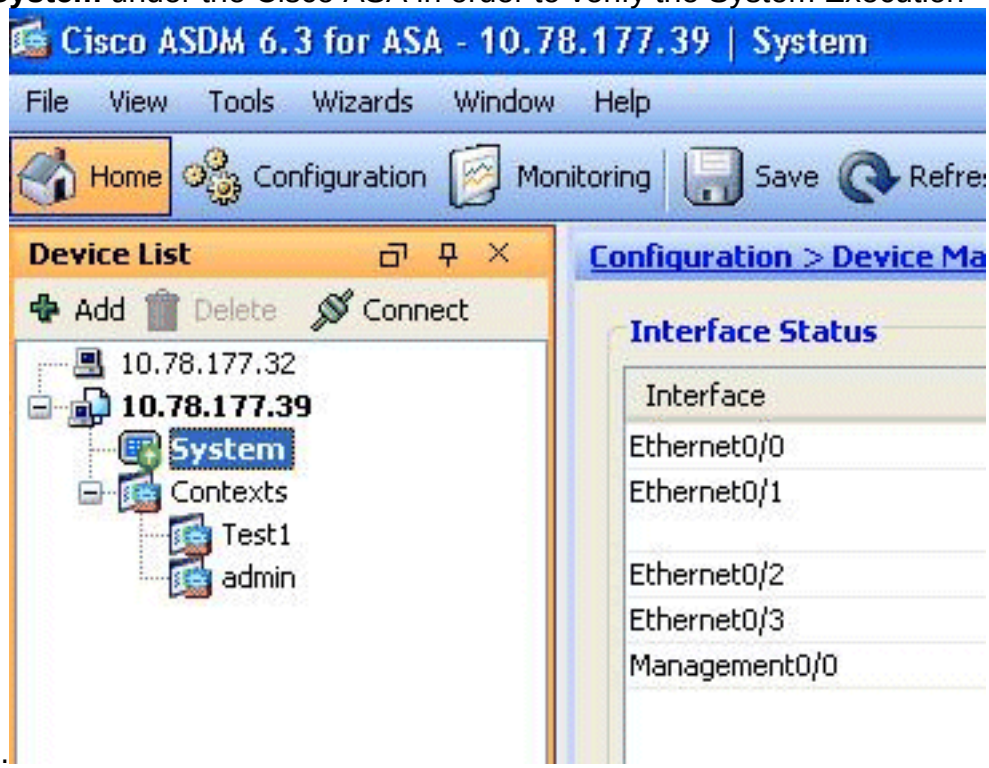
This document uses this network setup:



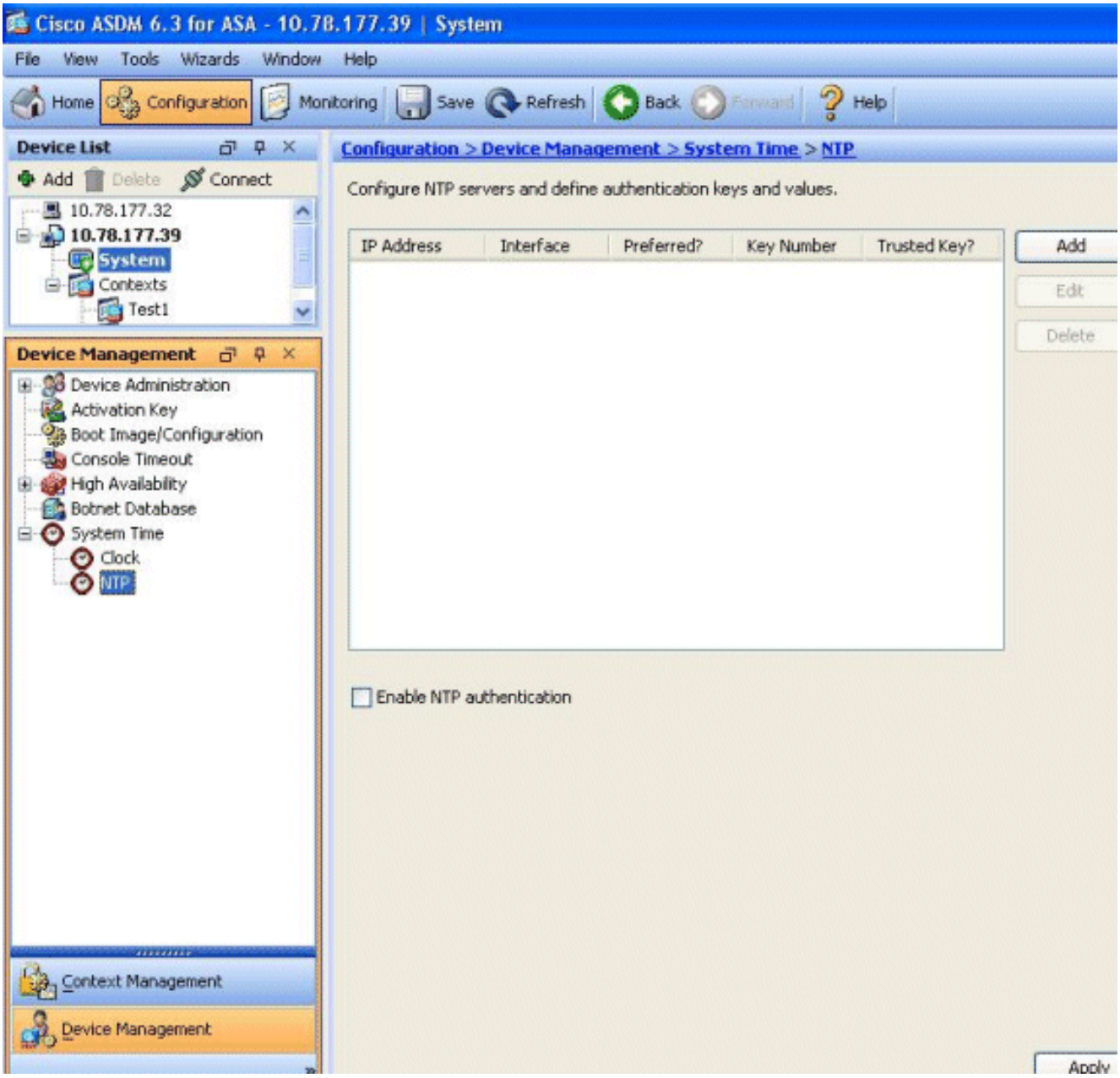
ASDM Configuration

Complete these steps in order to configure the ASDM:

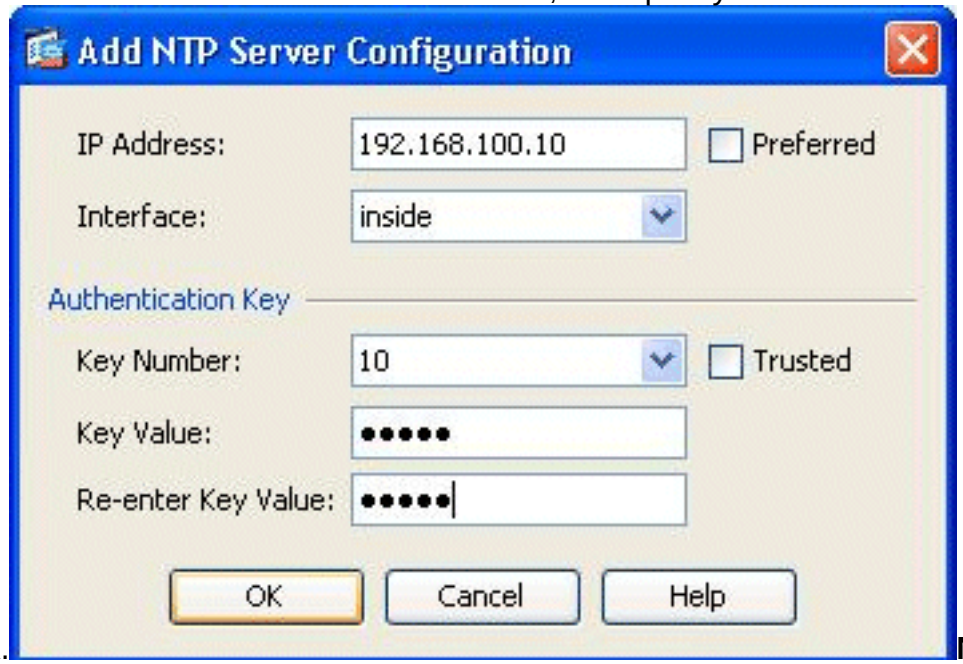
1. Click **System** under the Cisco ASA in order to verify the System Execution Space.



2. Go to **Configuration** > **Device Management** > **System Time** > **NTP**, and click **Add**.



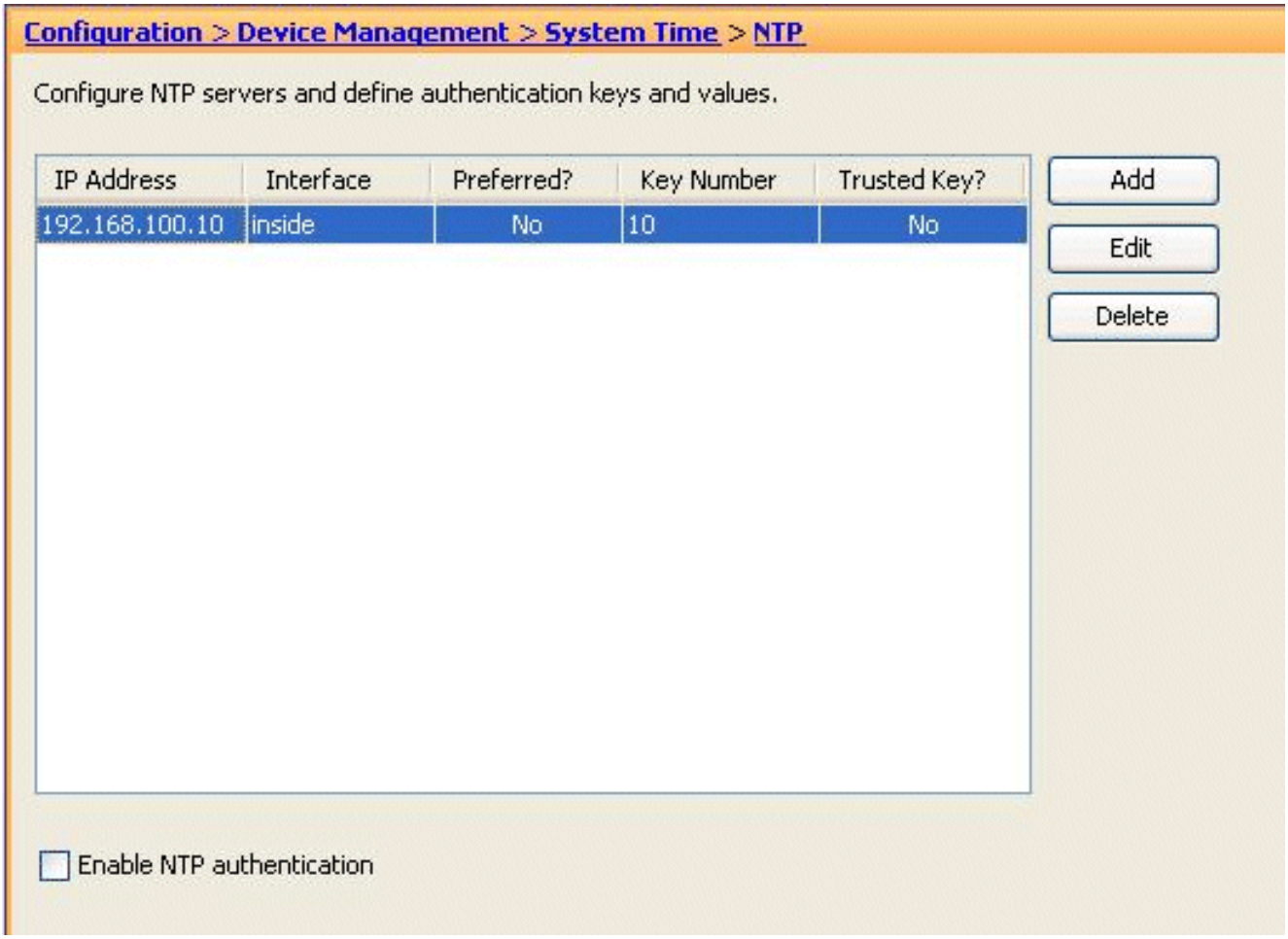
3. The Add NTP Server Configuration window is displayed. Specify the IP address of the interface that is associated with the NTP Server, and specify the Authentication Key details.



Click **OK**. **Note:** NTP

Server details should be specified within the context System. However, since the System Execution Space does not include any interfaces in multiple context mode, you need to specify an interface name (that is, defined within the Admin context).

4. View the NTP Server details in this window:



This is the equivalent CLI configuration of the Cisco ASA, for your reference:

Cisco ASA

```
ciscoasa# show run : Saved : ASA Version 8.2(1) <system>
! terminal width 511 hostname ciscoasa enable password
2KFQnbNIdI.2KYOU encrypted no mac-address auto !
interface Ethernet0/0 ! interface Ethernet0/1 !
interface Ethernet0/2 ! interface Ethernet0/3 shutdown !
interface Management0/0 shutdown ! class default limit-
resource All 0 limit-resource ASDM 5 limit-resource SSH
5 limit-resource Telnet 5 ! ftp mode passive clock
timezone GMT 0 pager lines 10 no failover asdm image
disk0:/asdm-635.bin asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin allocate-interface Ethernet0/0 allocate-interface
Ethernet0/1 allocate-interface Ethernet0/2 allocate-
interface Ethernet0/3 config-url disk0:/admin.cfg !
context Test1 allocate-interface Ethernet0/1 allocate-
interface Ethernet0/3 config-url disk0:/Test1.cfg ! !---
This command is used to set a key to !--- authenticate
with an NTP server. ntp authentication-key 10 md5 * !---
This command is used to configure the !--- NTP server IP
address and the interface associated. ntp server
192.168.100.10 source inside username Test password
I2xAvC8b372aLGtP encrypted privilege 15 username Cisco
password dDFIeex1zkFMaVXs encrypted privilege 15 !---
```

```
Output suppressed. ! prompt hostname context
Cryptochecksum:ae65e1f96123ea351ca1086c22f3ebc7 : end
ciscoasa#
```

FWSM in Multiple Context Mode as an NTP Client

Cisco Firewall Service Module (FWSM) does not support the NTP configuration separately. The FWSM clock is automatically synchronized with the clock of the Catalyst Switch as the module is booting up. If the Catalyst Switch itself is synchronized to an NTP server, the FWSM will inherit that clock.

Verify

Use this section in order to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ntp status** - Shows the status of each NTP association.`ciscoasa# show ntp status Clock is synchronized, stratum 10, reference is 192.168.100.10 nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6 reference time is d3a93668.7b6b6155 (11:41:28.482 GMT Thu Jul 12 2012) clock offset is -2.0439 msec, root delay is 1.48 msec root dispersion is 3894.03 msec, peer dispersion is 3891.95 msec`
- **show ntp associations** - Shows the information regarding the NTP association.`ciscoasa# show ntp associations address ref clock st when poll reach delay offset disp *~192.168.100.10 127.127.7.1 9 7 64 7 1.5 -2.04 3892.0 * master (synced), # master (unsynced), + selected, - candidate, ~ configuredciscoasa# show ntp associations detail 192.168.100.10 configured, our_master, sane, valid, stratum 9 ref ID 127.127.7.1, time d3aa5d7a.d8cf2704 (08:40:26.846 GMT Fri Jul 13 2012) our mode client, peer mode server, our poll intvl 1024, peer poll intvl 1024 root delay 0.00 msec, root disp 0.03, reach 377, sync dist 16.602 delay 1.71 msec, offset 1.3664 msec, dispersion 15.72 precision 2**16, version 3 org time d3aa5d8a.68391cb8 (08:40:42.407 GMT Fri Jul 13 2012) rcv time d3aa5d8a.6817b624 (08:40:42.406 GMT Fri Jul 13 2012) xmt time d3aa5d8a.67a3f2da (08:40:42.404 GMT Fri Jul 13 2012) filtdelay = 1.71 1.60 1.57 1.68 1.59 1.66 1.65 1.65 filtoffset = 1.37 1.41 1.50 1.52 1.63 1.61 1.56 1.53 filterror = 15.63 31.25 46.88 62.50 78.13 93.75 109.38 125.00`

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Error: Peer/Server Clock unsynchronized

Cisco ASA is not synchronizing with the NTP server, and this error message is received:

```
NTP: packet from 192.168.1.1 failed validity tests 20
 Peer/Server Clock unsynchronized
```

Solution:

Enable the NTP debugs, and verify this output in detail:

```
ciscoasa(config)# NTP: xmit packet to 192.168.1.1:
   leap 3, mode 3, version 3, stratum 0, ppoll 64
```

It looks like the NTP Server is configured with a stratum zero, which is specified as "Unspecified" as per RFC 1305 .

In order to resolve this error, define the stratum number of the NTP server between 6-10.

Problem: Unable to Synchronize clock with NTP server

The Cisco ASA was configured as an NTP client, but the synchronization does not work and this output is received:

```
ciscoasa# show ntp status Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6 reference
time is d3a93395.388e423c (11:29:25.220 GMT Thu Jul 12 2012) clock offset is -
4050.4142 msec, root delay is 1.21 msec root dispersion is 19941.07 msec, peer
dispersion is 16000.00 msec
```

Solution:

In order to resolve this issue, verify these items:

- Check whether the NTP Server is reachable from Cisco ASA. Perform the ping test and verify the routing.
- Make sure the Cisco ASA configuration is intact and matches the parameters of the NTP Server.
- Enable the NTP **debug** commands in order to dig further.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug ntp packet** - Shows messages about NTP packets.
- **debug ntp event** - Shows messages about NTP events.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances Product Support**
- **Example NTP Configuration for High Availability Catalyst 6000 Switch**
- **NTPv3 RFC 1305**
- **Technical Support & Documentation - Cisco Systems**