Release Notes for the Cisco ASA Device Package Software, Version 1.2(5.21) for ACI

Revised: May 3, 2016
Published: May 3, 2016

This document contains release information for the Cisco ASA Device Package software, Version 1.2(5.21) for ACI, and includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Supported ASA Models

The following table lists the supported ASA models.

ASA Model	Software Version
ASA 5500-X (5512 through 5555)	ASA software Version 8.4(x) and later
ASA 5585-X (SSP 10 through SSP 60)	
ASAv	

Supported APIC Versions

Cisco ASA Device Package Software supports only the version of APIC that it is shipped with.

New Features in 1.2(5.21)

Three caveats were resolved in release 1.2(5.21). For details, see the "Resolved Caveats in the ASA Device Package Version 1.2(5.21)" section on page 5.

New Features in 1.2(5.5)

This release includes support for Cisco TrustSec.

Cisco TrustSec enables you to avoid the extensive manual maintenance required for traditional network segmentation, which uses VLANs and access control lists (ACLs) that are based on IP addresses. Cisco TrustSec simplifies network segmentation by dynamically organizing machines into logical groups, called security groups, and enabling security policies to be written using security group tags.

Cisco TrustSec uses the Cisco Identity Services Engine as a centralized policy management platform to gather contextual data about who and what is accessing your network. You can then use this information to create security groups and to assign access rights based on role, function, location, and other criteria. For more information about Cisco TrustSec, see Cisco TrustSec "At-a-Glance".

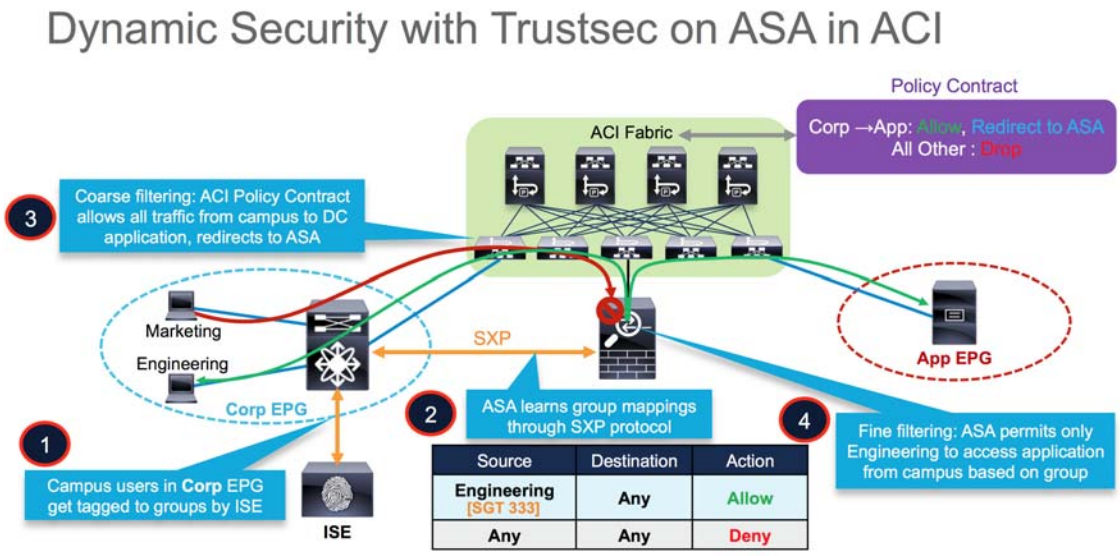
The following support for the Cisco TrustSec functionality is included in ASA Device Package 1.2(5):

- AAA server group - Configures the AAA server parameters for the ASA to communicate with the ISE server.
  - Server group used for environment data retrieval, specifically the Security Group table from ISE
- Configuring the Security Exchange Protocol (SXP) involves enabling the protocol in the ASA and setting the following values for SXP:
  - The source IP address of SXP connections and SXP peer IP address and their role
  - The authentication password between SXP peers
  - The retry interval for SXP connections
  - The Cisco TrustSec SXP reconcile period

- Configuring SGT-to-IP address role-based mapping manually
- Security groups in an access control entry to leverage SGT-to-IP mapping
- Security object group

In the example below, only IP addresses that belong to the Security Group “Engineering” are allowed to access EPG App, while denying all other Security Groups.

Figure 1-1 Example Configuration



Restrictions

The PAC file from the ISE will need to be imported as part of pre-provisioning. Refreshing the environment data from the ISE will need to be done out-of-band.

For details about Configuring the ASA to Integrate with Cisco TrustSec, see: http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/aaa_trustsec.pdf

Note Cisco Application Centric Infrastructure (ACI) does not have native support of the Security-group eXchange Protocol (SXP). Therefore, in order to use TrustSec in ASA for ACI, you must have an SXP-capable switch.

Cisco ACI is a distributed, scalable, multi-tenant infrastructure with external end-point connectivity controlled and grouped through application-centric policies. SXP is the protocol used to propagate the IP-to-SGT mapping database across network devices that do not have SGT-capable hardware support. The Cisco Application Policy Infrastructure Controller (APIC) is a unified point of automation, management, monitoring, and programmability for the Cisco ACI.

Tip To use TrustSec in ASA for ACI, changes to your network topology might be required. For details about the required topology and configuration examples, see the Cisco listing page shown below. This information will be available by March 14, 2016.

Related Documentation

For more information about the features and benefits of Cisco TrustSec and Cisco ASA Device Package Software for ACI, see:

- Listing page for all APIC documentation
- *Navigating the Cisco ASA Series Documentation*
- Cisco Application Centric Infrastructure Security Solutions
- Cisco TrustSec "At-a-Glance"

Important Notes

Pay attention to the following important notes:

- The ASAv does not support multiple context mode.
- ACE with dynamic EPG requires ASA image 9.3.2 or later.

APIC 1.2(x) and ASA 9.3(1)

If you are running APIC 1.2(x) with ASA 9.3(1), which has a default SSL configuration, you will see the following error:

```
*Major script error : Connection error : [SSL:SSLV3_ALERT_HANDSHAKE_FAILURE] sslv3 alert
handshake failure(_ssl.c:581)*
```

The workaround is to have **ssl encryption aes128-sha1** configured on the ASA, or to upgrade the ASA to version 9.3(2) or later.

The Policy Manager Lock Ups when the Configuration for BGP Peering for the Service Appliance is Incomplete

Symptom The Policy Manager crashes when the l3Out that is used for BGP peering for the service appliance has an incomplete configuration (CSCuw03425).

Conditions The l3Out used for BGP peering for the service appliance is missing l3extRsNodeL3OutAtt.

Workaround Make sure that the l3Out contains l3extRsNodeL3OutAtt. This problem will be fixed in a subsequent release.

The following shows the BGP XML example with l3extRsNodeL3OutAtt:

```
<polUni>
    <fvTenant name="tenant1">
        <l3extOut name="StaticExternal">
            <l3extLNodeP name="bLeaf-101">
                <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="190.0.0.11">
                    <ipRouteP ip="50.50.50.0/24">
                        <ipNexthopP nhAddr="40.40.40.102/32"/>
```

```
                    </ipRouteP>
                </l3extRsNodeL3OutAtt>
                <l3extLIfP name="portIf">
                    <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/15]" ifInstT="ext-svi"
encap="vlan-3843" addr="40.40.40.100/28" mtu="1500"/>
                </l3extLIfP>
            </l3extLNodeP>
            <l3extInstP name="ExtInstP">
                 <l3extSubnet ip="50.50.50.0/24" scope="export-rtctrl"/>
            </l3extInstP>
            <l3extRsEctx tnFvCtxName="tenant1ctx1"/>
        </l3extOut>
    </fvTenant>
</polUni>
```

Installing the Software

To upgrade, you do not need to remove the previous package if your APIC release has the fix for CSCuv4353. Otherwise, to upgrade from an older version to a newer, you need to remove the old version from APIC first, then install the new version.

To install the ASA Device Package software, see *Cisco ASA Quick Start Guide for APIC Integration, 1.2* for instructions.

Downloading the Software from Cisco.com

If you have a Cisco.com login, you can obtain the ASA Device Package image from the following website:

https://software.cisco.com/download/release.html?i=!y&mdfid=286119613&softwareid=286279676&release=1.2.4.1&os=

Bug Search

If you are a registered Cisco.com user, view more information about each caveat using Bug Search at the following website:

https://tools.cisco.com/bugsearch

Resolved Caveats in the ASA Device Package Version 1.2(5.21)

The following table contains the resolved caveats in ASA Device Package Version 1.2(5.21):

Caveat	Description
CSCuz07266	Trustsec role-based sgt-map command will fail if upgraded to ASA 9.6.1
CSCuz08407	AVS BZMR2 - ASAv VMs lost access after deleting the device
CSCuy77421	ASA DP needs to support timeout sctp

Resolved Caveats in the ASA Device Package Version 1.2(5.5)

The following table contains the resolved caveats in ASA Device Package Version 1.2(5):

Caveat	Description
CSCux50528	ASA ACI device package can not find user context in cluster multi-cix
CSCuw58946	Brazos EFT: regression with shared BD
CSCux80570	asa-dp: take care of forward reference in object-group in ASA 9.3(1)
CSCux98333	Global inspection policy is getting deleted during APIC audit

Related Documentation

For additional information about the Cisco ASA, see *Navigating the Cisco ASA Series Documentation*.

For additional information about the Cisco APIC, see the APIC Documentation website and the Cisco Application Centric Infrastructure Security Solution website.

For additional information about Cisco TrustSec, see Cisco TrustSec "At-a-Glance".

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.