

PKI Split VRF in Trustpoint

The PKI Split VRF in Trustpoint feature allows you to configure a VPN Routing and Forwarding (VRF) for certificate enrollment and revocation.

- Information About PKI Split VRF in Trustpoint, on page 1
- How to Configure PKI Split VRF in Trustpoint, on page 2
- Configuration Examples for PKI Split VRF in Trustpoint, on page 3
- Additional References for PKI Split VRF in Trustpoint, on page 3
- Feature Information for Overview of Cisco TrustSec, on page 4

Information About PKI Split VRF in Trustpoint

Overview of PKI Split VRF in Trustpoint

The PKI Split VRF in Trustpoint feature allows you to configure VPN Routing and Forwarding (VRF) for certificate enrollment and for certificate revocation list (CRL) checking. The VRF is configured in the enrollment profile using the **enrollment url** command under the **crypto pki profile enrollment** command to attach the enrollment profile to a trustpoint. You can configure the same VRF for enrollment and CRL or configure different VRFs. Based on the configuration (enrollment or revocation), the corresponding VRF is selected and Simple Certificate Enrollment Protocol (SCEP) request is sent via the respective VRF.

To configure enrollment and CRL via different routing paths, you must configure the enrollment url command using the **crypto pki profile enrollment** command. This configured VRF acts as an enrollment VRF and the enrollment request goes via that VRF. However, the CRL uses the global VRF configured in the trustpoint using the

If no VRF is configured in the **enrollment url** command, the enrollment takes global enrollment that is configured in the **crypto pki trustpoint** command.

How to Configure PKI Split VRF in Trustpoint

Configuring the Split VRF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki profile enrollment** *label*
4. **enrollment url** *url* [**vrf** *vrf-name*]
5. **exit**
6. **show crypto pki profile**
7. **show crypto pki trustpoint**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki profile enrollment** *label* **Example:** `Device(config)# crypto pki profile enrollment pki_profile`	Defines an enrollment profile and enters ca-profile-enroll configuration mode. • *label* —Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command.
Step 4	**enrollment url** *url* [**vrf** *vrf-name*] **Example:** `Device(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1`	Specifies the URL and the VPN Routing and Forwarding (VRF) of the CA server to which to send certificate enrollment requests via HTTP or TFTP.
Step 5	**exit** **Example:** `Device(ca-profile-enroll)# exit`	Exits ca-profile-enroll configuration mode. • Enter this command a second time to exit global configuration mode.
Step 6	**show crypto pki profile** **Example:**	(Optional) Displays information about PKI profile.

	Command or Action	Purpose
	`Device# show crypto pki profile`	
Step 7	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays information about PKI trustpoints.

Configuration Examples for PKI Split VRF in Trustpoint

Example: Configuring the PKI Split VRF in Trustpoint

Enrollment and Certificate Revocation List Via Same VRF

The following example shows how to configure the enrollment and certificate revocation list (CRL) via the same VRF:

```
crypto pki trustpoint trustpoint1
 enrollment url http://10.10.10.10:80
 vrf vrf1
 revocation-check crl
```

Enrollment and Certificate Revocation List Via Different VRF

The following example shows how to configure the enrollment and certificate revocation list (CRL) via different VRF:

```
crypto pki profile enrollment pki_profile
 enrollment url http://10.10.10.10:80 vrf vrf2

crypto pki trustpoint trustpoint1
 enrollment profile pki_profile
 vrf vrf1
 revocation-check crl
```

Additional References for PKI Split VRF in Trustpoint

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
Recommended cryptographic algorithms	Next Generation Encryption

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Overview of Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.