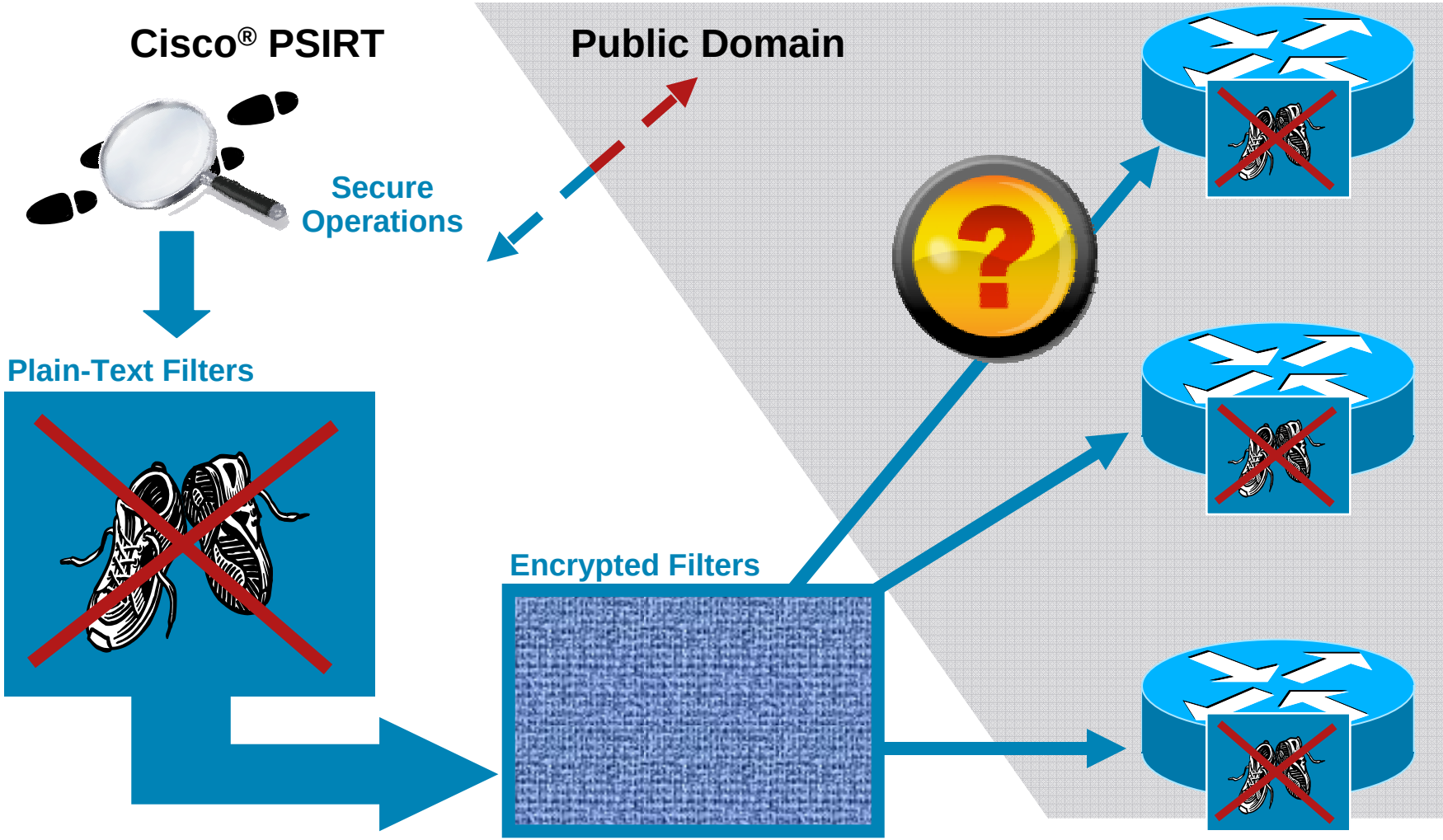
Cisco Automated IOS Protection Solution

Solution Summary

- Along with applicable advisory announcements by the Cisco® Product Security Incident Response Team (PSIRT), a package of traffic filters will be posted to Cisco.com
- Filters are designed to protect the router itself by detecting and stopping potential exploits of software vulnerabilities announced by Cisco PSIRT
- Packages posted also contain Cisco IOS® Software versions to which the filters apply
- Each traffic filter in the packages is encrypted and can be decrypted only by Cisco routers configured for this automated self-protection mechanism
- As an extra security measure, packages contain a checksum also digitally signed by Cisco
- Routers will apply only filters applicable to the Cisco IOS Software version running
- Filters may be applied to traffic passing through selected or all interfaces configured on the router
- Filter packages may be do downloaded manually or in an automated (periodic) fashion from a local server or directly from Cisco.com
- Solution requires a Security license on the Cisco Integrated Services Routers Generation 2 (ISR G2) Family of routers

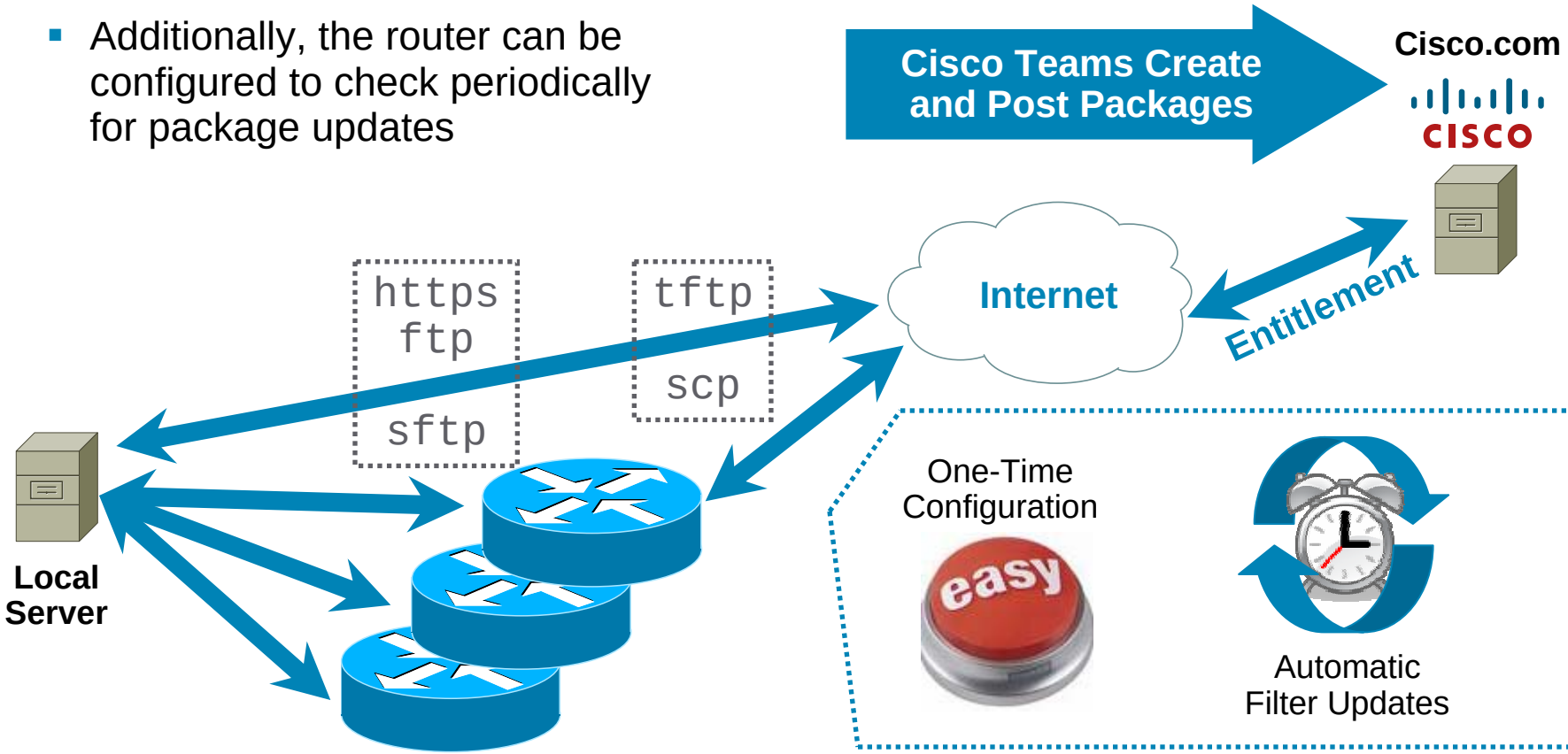
Solution Overview (1 of 3)



Solution Overview (2 of 3)

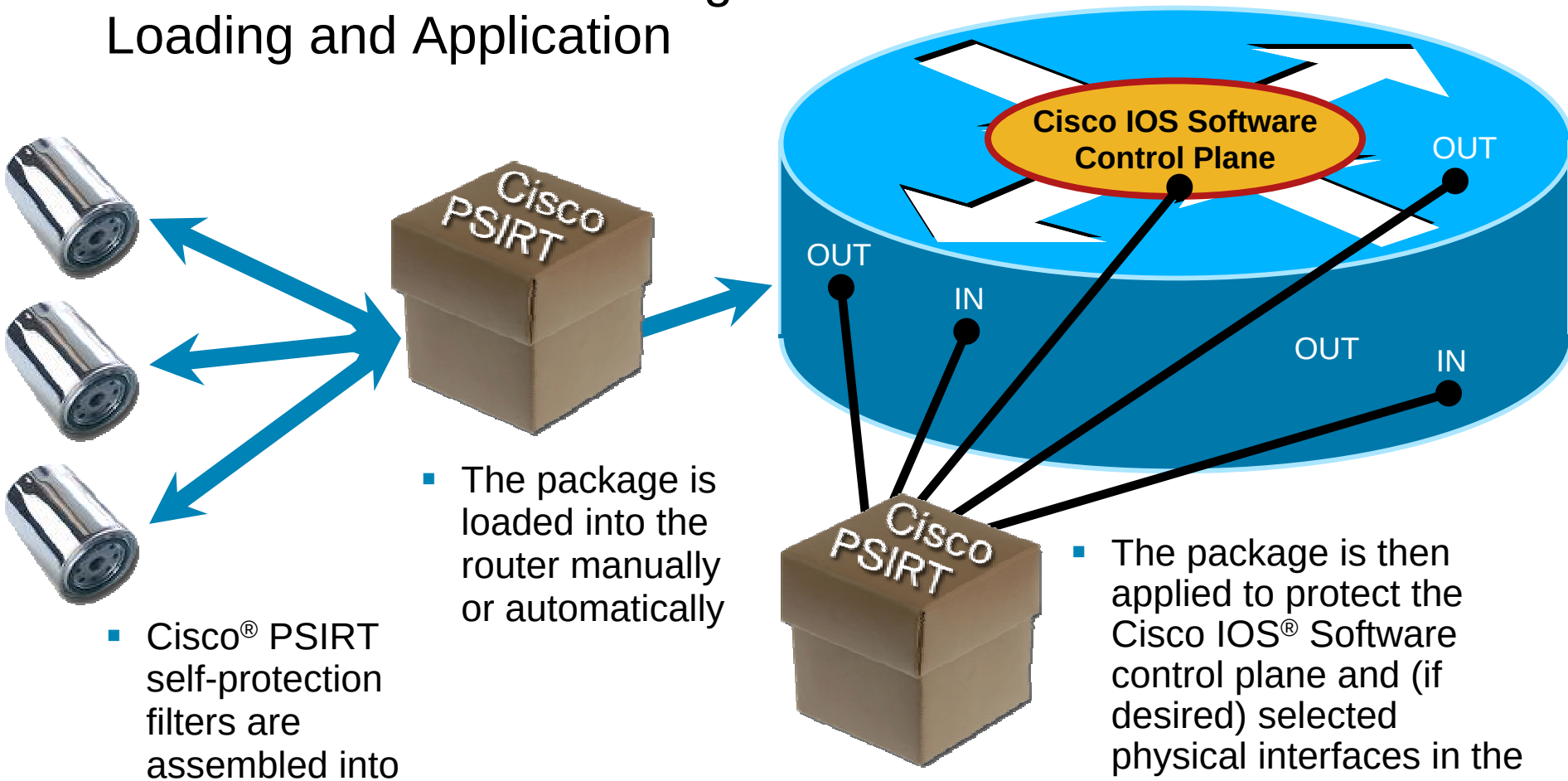
Cisco PSIRT Filter Packaging

- With only one-time configuration, a user can deploy Cisco® PSIRT self-protection filters on a router
- Additionally, the router can be configured to check periodically for package updates
- Router can be configured to pull package updates automatically from Cisco or any server



Solution Overview (3 of 3)

Cisco PSIRT Filter Package Loading and Application



- Cisco® PSIRT self-protection filters are assembled into a package
- The package is loaded into the router manually or automatically
- The package is then applied to protect the Cisco IOS® Software control plane and (if desired) selected physical interfaces in the inbound and outbound traffic directions

Possible Use of Cisco PSIRT Filter Package Loading Process