CISCO IOS IPSEC HIGH AVAILABILITY TECHNICAL OVERVIEW

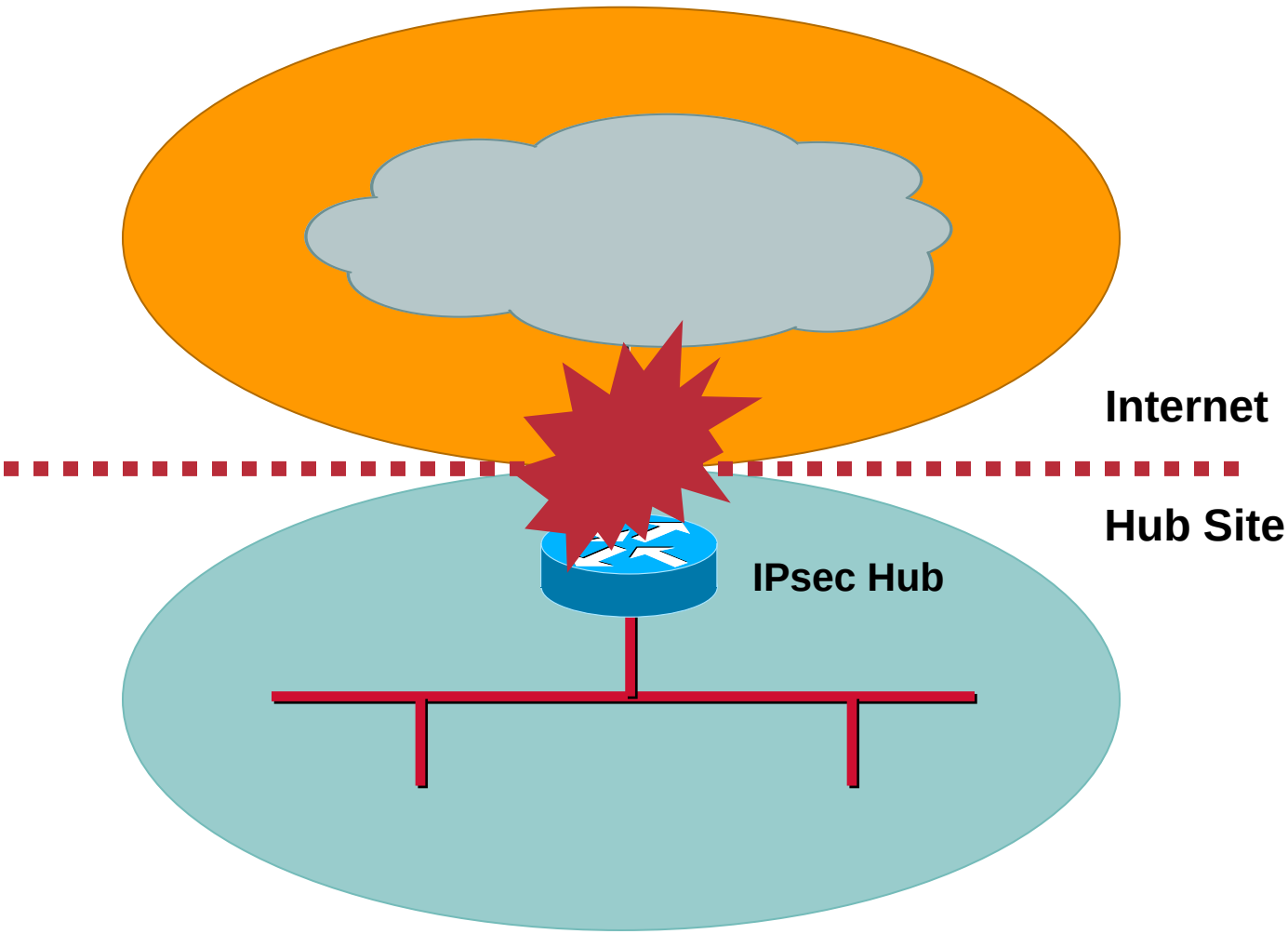
SECURITY TECHNOLOGY GROUP

SEPTEMBER 2004

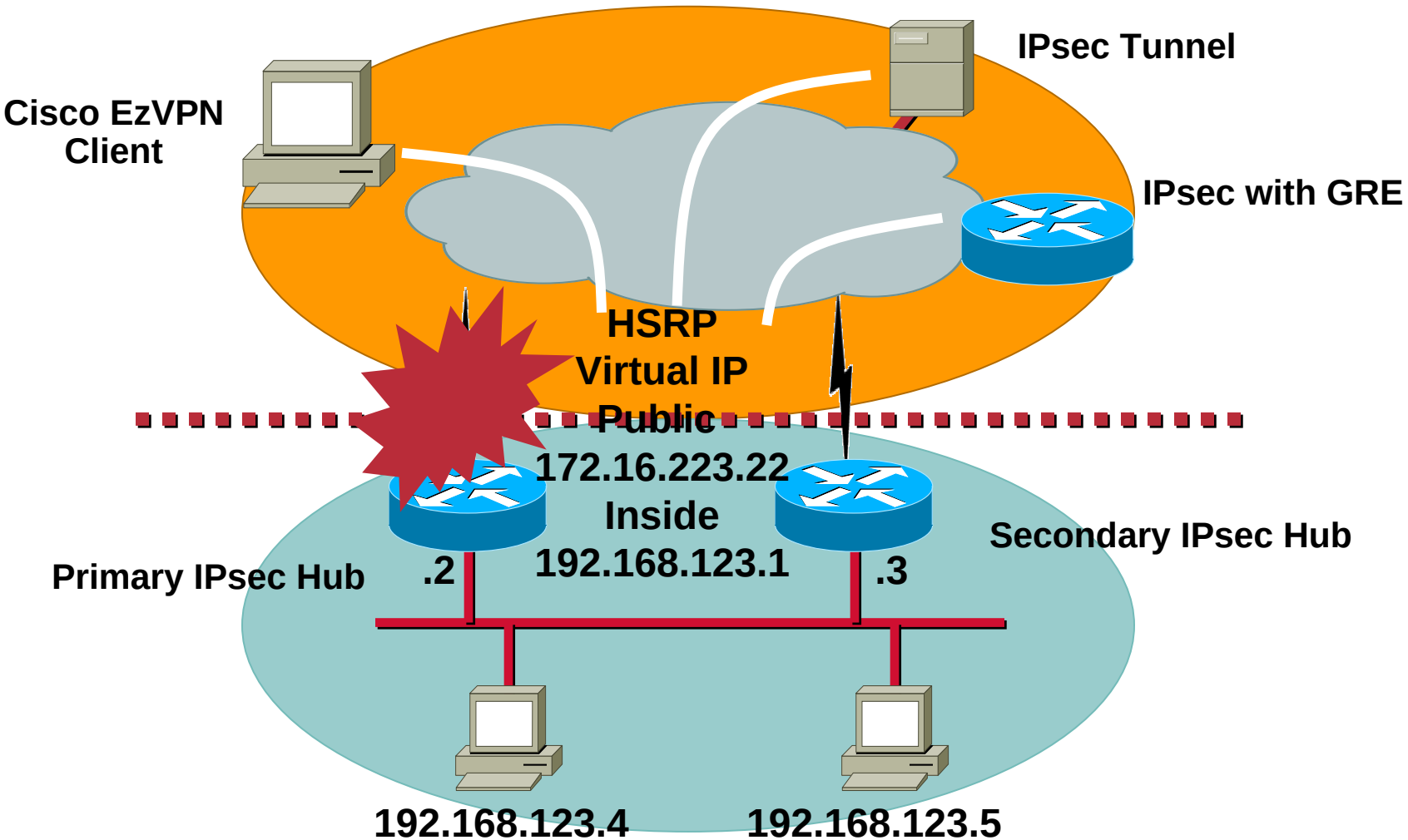
Agenda

- **Problem definition**
- **IPsec High Availability solution review**
- **Cisco IOS IPsec Stateful Failover in Cisco IOS® Software Release 12.3(11)T**

Critical Points of Failure



IPsec Redundancy with Hot Standby Router Protocol

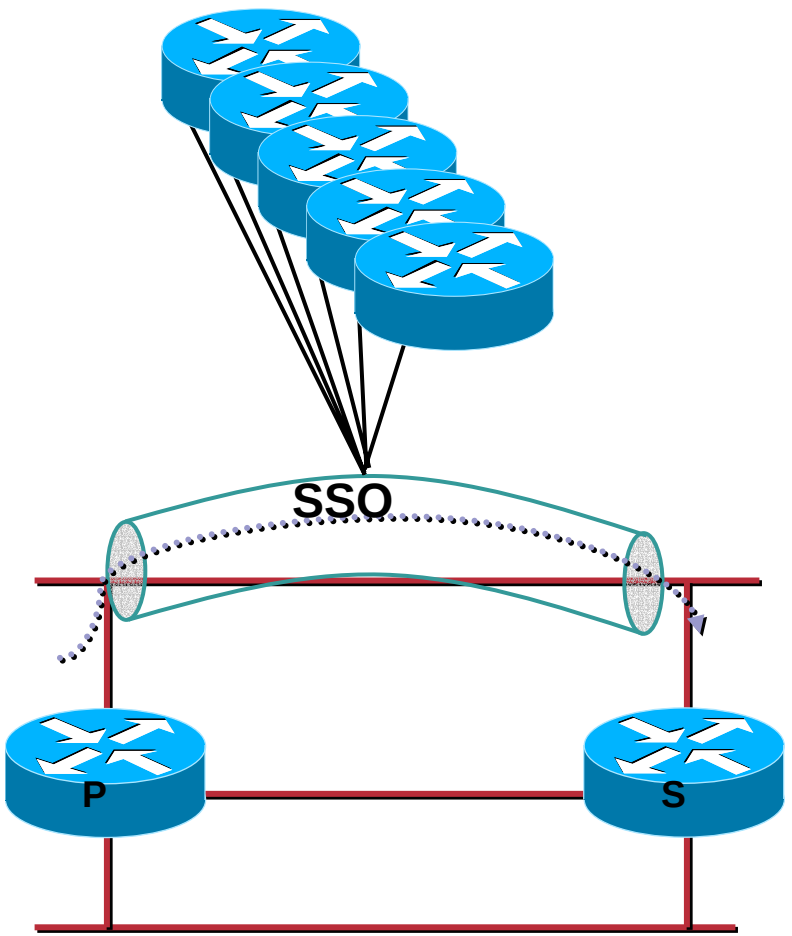


IPsec Stateful Failover Adds Redundancy for Crypto SA

- Supports dynamic and static Peers
- Provides transparent failover for end users
- Entries created on primary IPsec Hub router are distributed to backup IPsec Hub router
- Messages exchanged between IPsec High Availability peers over SSO protocol
- Primary IPsec HA router that created the entries is responsible for timing the entries
- IPsec Stateful Failover enables session resiliency during critical failure

High Availability Solution
Cisco IOS IPsec Stateful Failover

- IPsec Stateful Failover greatly improves failover time compared to the stateless IPsec / Hot Standby Routing Protocol (HRRP) failure
- Stateful Switchover (SSO) syncs ISAKMP and IPsec SA database between HSRP active and standby routers
- Use a dedicated link between the two HSRP routers for SSO exchange



Prerequisites:

- Requires two identical routers for primary and secondary hub, same CPU, memory, configuration and encryption accelerators, identical version of the Cisco IOS Software
- Available on Cisco 3700 and 7200 Series, and Cisco 7301 Router
- Supports VPN Acceleration Module (VAM), VAM2, AIM-VPN/HPII hardware accelerators

IPsec Stateful Failover in Release 12.3(11)T

- **Active/standby stateful failover arrives in Release 12.3T**
- **Based on SSO infrastructure, rather than SSP**
- ***Supports* EasyVPN/RA, GRE/IPsec, tunnel protection, and VRFs**
- **PSK only (no PKI)**
- **Available on Cisco 3700 and 7200 Series**
  - **Support for the Cisco 7301 Router will be added in the future**
- **Failover times in the range of 2 seconds (with 1 second HSRP hold time *and* BGP update)**
  - **Can be tuned for faster (sub-second) times**

For Additional Information

- **Cisco IOS IPsec**

  www.cisco.com/go/ipsec/

- **Release 12.3(11)T**

  www.cisco.com/go/release123t/

- **Technical Documentation**

  www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guides_list.html