Web Services Security Configuration Challenges

Sanjai Narain
Senior Research Scientist
Telcordia Technologies
narain@research.telcordia.com
(732) 699 2806

Prepared for IFIP WG 10.4, January 26-30
Rincon, PR

Deploying Web Services Security Infrastructure

Challenge is assembling building blocks to satisfy end-to-end requirements on security *and* availability

Some problems

How to precisely specify this plan? Constraints are *global*.

How to reconcile constraints, and synthesize component configurations?

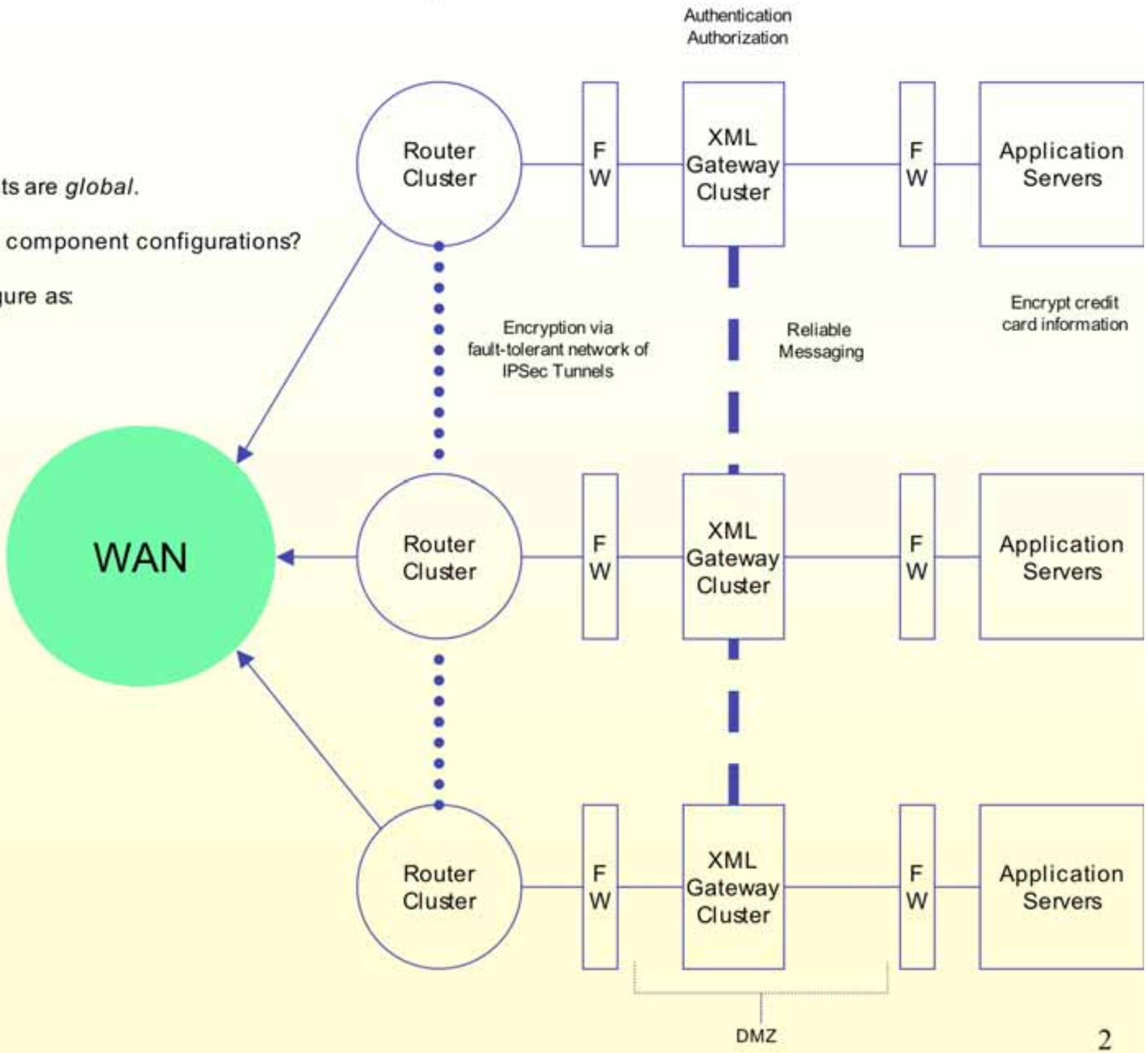
New site needs to be added. How to reconfigure as:
- Requirements change?
- New site is added or deleted?

How to reason about this?
- How much defense in depth is there?
- Are there single points of failure?

How to diagnose configuration errors?

How to troubleshoot these?

How to sequence configurations?



There is no theory of configuration

What are intellectual processes of system administrators?

Language to specify system configuration logic:
requirements on security, functionality, fault-tolerance...

How much defense in depth in a system?
Is there a single point of failure?

Configuration Synthesis | Requirement Strengthening | Component Adds & Deletes | Configuration Error Diagnosis | Configuration Error Fixing | Requirement Verification

These **reasoning** tasks are all manually performed. But reasoning with FOL is hard.

System requirements can't even be precisely specified, hence automation of reasoning tasks is impossible

Leads to high cost of infrastructure ownership

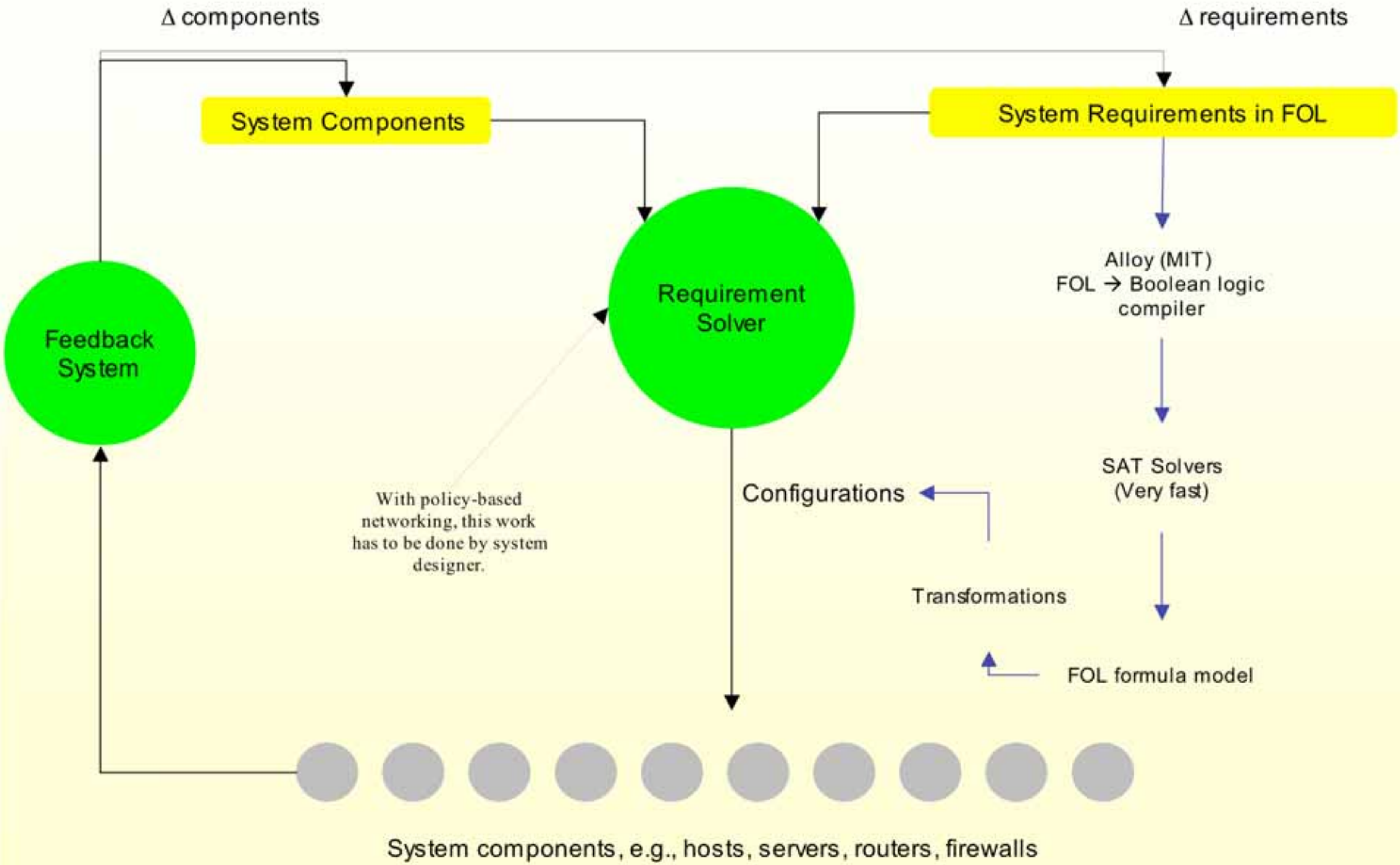
Configuration Sequencing

Components

Quotes

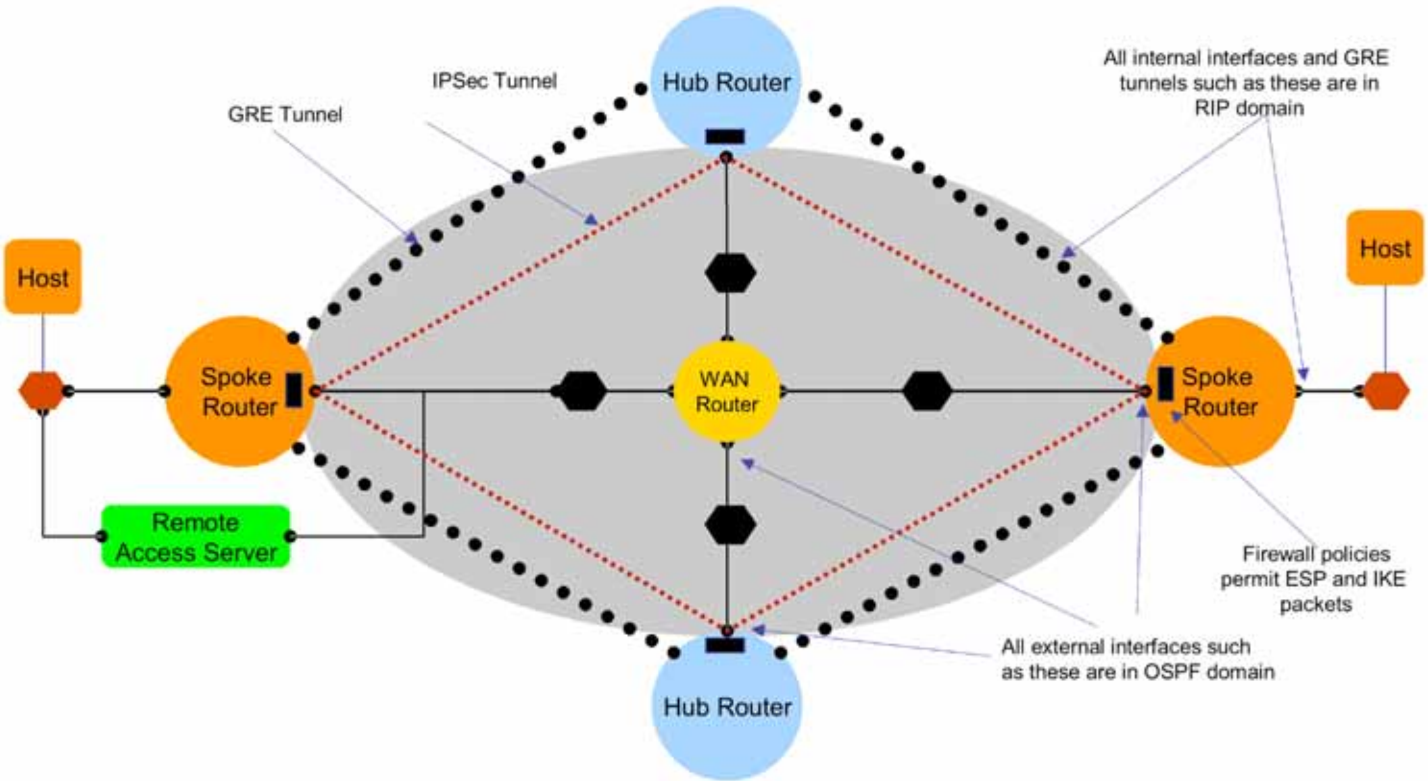
- ...operator error is the largest cause of failures...and largest contributor to time to repair ... in two of the three (surveyed) ISPs.......configuration errors are the largest category of operator errors. – David Oppenheimer, Archana Ganapathi, David A. Patterson. Why Internet Services Fail and What Can Be Done About These? *Proceedings of 4th Usenix Symposium on Internet Technologies and Systems (USITS '03*), 2003.
  – http://roc.cs.berkeley.edu/papers/usits03.pdf
- Although setup (of the trusted computing base) is much simpler than code, it is still complicated, it is usually done by less skilled people, and while code is written once, setup is different for every installation. So we should expect that it's usually wrong, and many studies confirm this expectation. – Butler Lampson, Computer Security In the Real World. *Proceedings of Annual Computer Security Applications Conference*, 2000.
  – http://research.microsoft.com/lampson/64-SecurityInRealWorld/Acrobat.pdf
- Consider this: ….the complexity [of computer systems] is growing beyond human ability to manage it….the overlapping connections, dependencies, and interacting applications call for administrative decision-making and responses faster than any human can deliver. Pinpointing root causes of failures becomes more difficult. –Paul Horn, Senior VP, IBM Research. Autonomic Computing: IBM's Perspective on the State of Information Technology.
  – http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf
- 65% of attacks exploit configuration errors. – British Telecom/Gartner Group. http://www.btglobalservices.com/business/global/en/products/docs/28154_219475secur_bro_single.pdf
- IP/VPN *services* market $18 billion in 2003. – Infonetics http://www.tekrati.com/T2/Analyst_Research/ResearchAnnouncementsDetails.asp?Newsid=3271

New Concept: Requirement Solver



Fault-Tolerant VPN

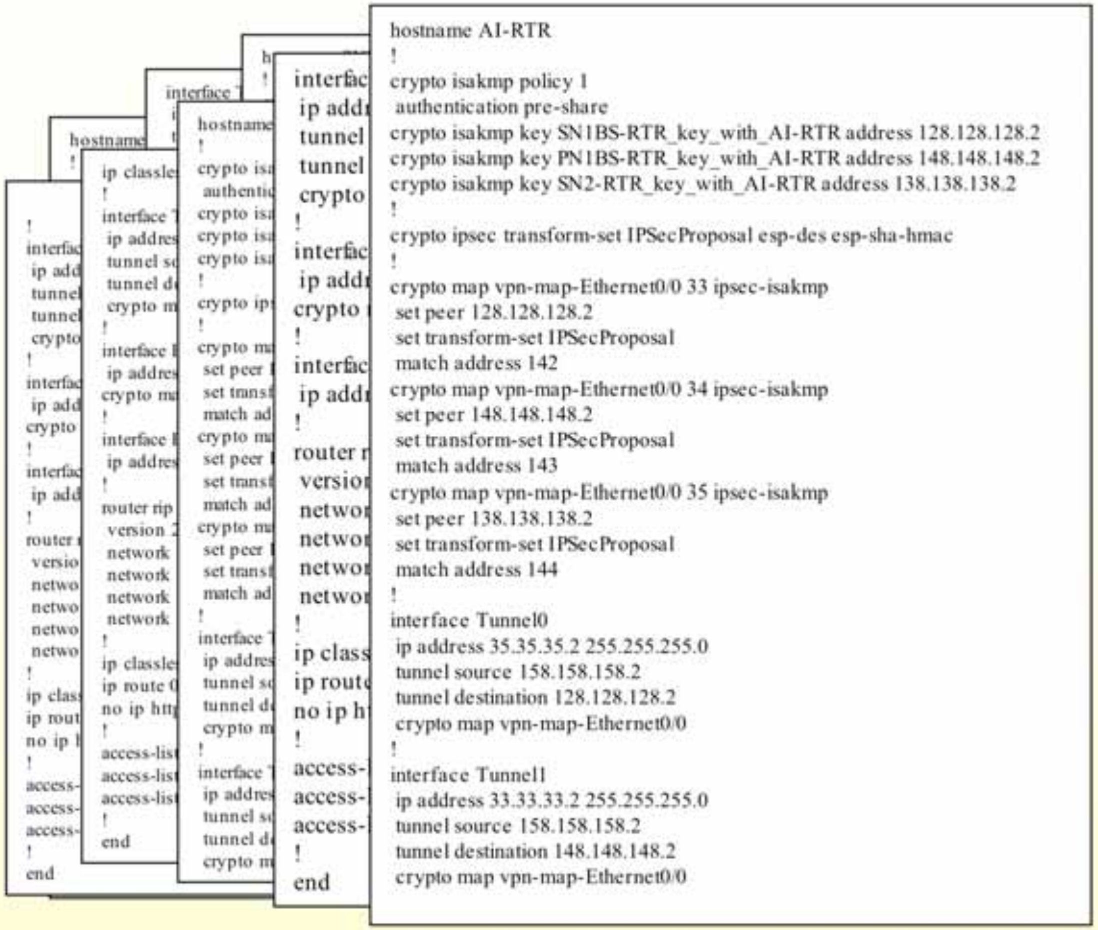
Illustrates composition of FT systems into larger FT system



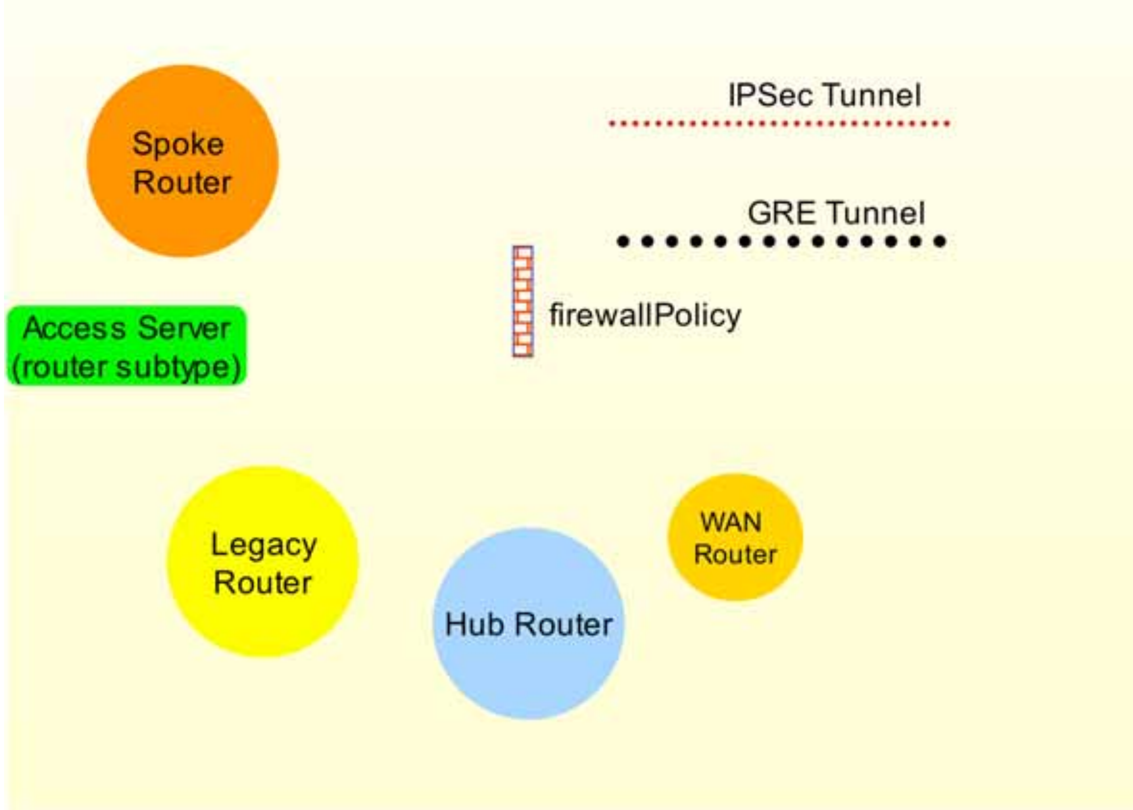
- Full mesh of IPSec tunnels does *not* scale
- Linearly-scaling solution can have single point of failure

Current VPN Configuration Process

New Cisco IOS configuration needs to be implemented at all VPN peer routers! For 4 node VPN that is more than 240 command lines



Network Components



Component Attributes

- interface
  - chassis: router
  - network: subnet
  - routing: routingDomain
- ipsecTunnel
  - local: externalInterface,
  - remote: externalInterface,
  - protocolToSecure: protocol
- greTunnel
  - localPhysical: externalInterface
  - remotePhysical:externalInterface
  - routing:routingDomain
- firewallPolicy
  - prot: protocol
  - action: permission
  - protectedInterface: physicalInterface
- ipPacket
  - source:interface,
  - destination:interface,
  - prot:protocol

List of Network Requirements

RouterInterfaceRequirements

1. Each spoke router has internal and external interfaces
2. Each access server has internal and external interfaces
3. Each hub router has only external interfaces
4. Each WAN router has only external interfaces

SubnettingRequirements

5. A router does not have more than one interface on a subnet
6. All internal interfaces are on internal subnets
7. All external interfaces are on external subnets
8. Every hub and spoke router is connected to a WAN router
9. No two non-WAN routers share a subnet

RoutingRequirements

10. RIP is enabled on all internal interfaces
11. OSPF is enabled on all external interfaces

GRERequirements

12. There is a GRE tunnel between each hub and spoke router
13. RIP is enabled on all GRE interfaces

SecureGRERequirements

14. For every GRE tunnel there is an IPSec tunnel between associated physical interfaces that secures all GRE traffic

AccessServerRequirements

15. There exists an access server and spoke router such that the server is attached in "parallel" to the router

FirewallPolicyRequirements

16. Each hub and spoke external interface permits esp and ike packets

Human administrators reason with these in different ways to synthesize initial network, then reconfigure it as operating conditions change.

Can we automate this reasoning?

Configuration Synthesis: Physical Connectivity and Routing

RouterInterfaceRequirements

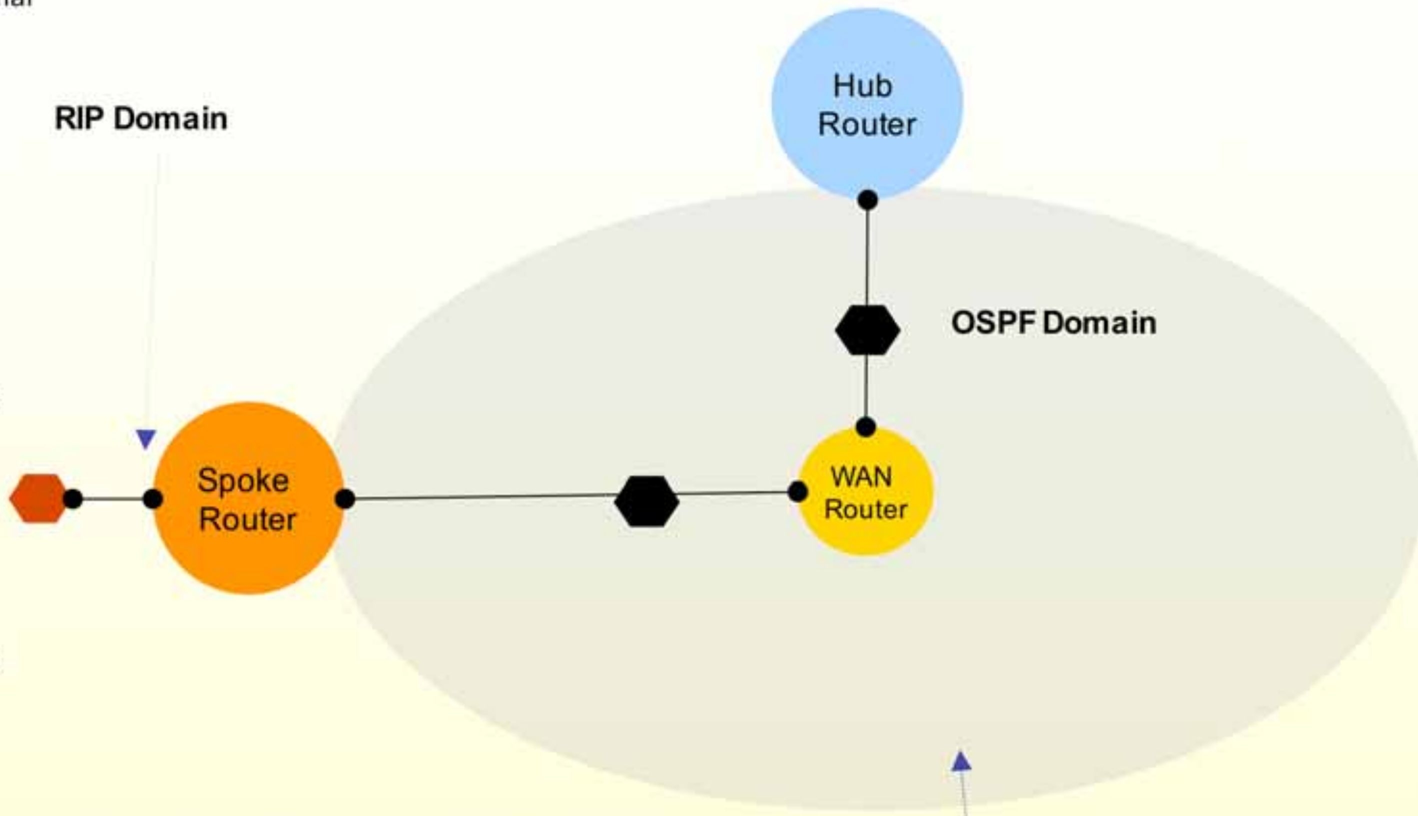
1. Each spoke router has internal and external interfaces
2. Each access server has internal and external interfaces
3. Each hub router has only external interfaces
4. Each WAN router has only external interfaces

SubnettingRequirements

5. A router does not have more than one interface on a subnet
6. All internal interfaces are on internal subnets
7. All external interfaces are on external subnets
8. Every hub and spoke router is connected to a WAN router
9. No two non-WAN routers share a subnet

RoutingRequirements

10. RIP is enabled on all internal interfaces
11. OSPF is enabled on all external interfaces



- To synthesize network, satisfy R1-R11 for
  - 1 hub router,
  - 1 WAN router,
  - 1 spoke router,
  - 1 internal subnet,
  - 2 external subnets
  - 1 internal interface,
  - 4 external interfaces,
  - RIP domain,
  - 1 OSPF domain

Requirement Solver generates solution. Note that Hub and Spoke routers are not directly connected, due to Requirement 9

Strengthening Requirement: Adding Overlay Network

RouterInterfaceRequirements

1. Each spoke router has internal and external interfaces
2. Each access server has internal and external interfaces
3. Each hub router has only external interfaces
4. Each WAN router has only external interfaces

SubnettingRequirements

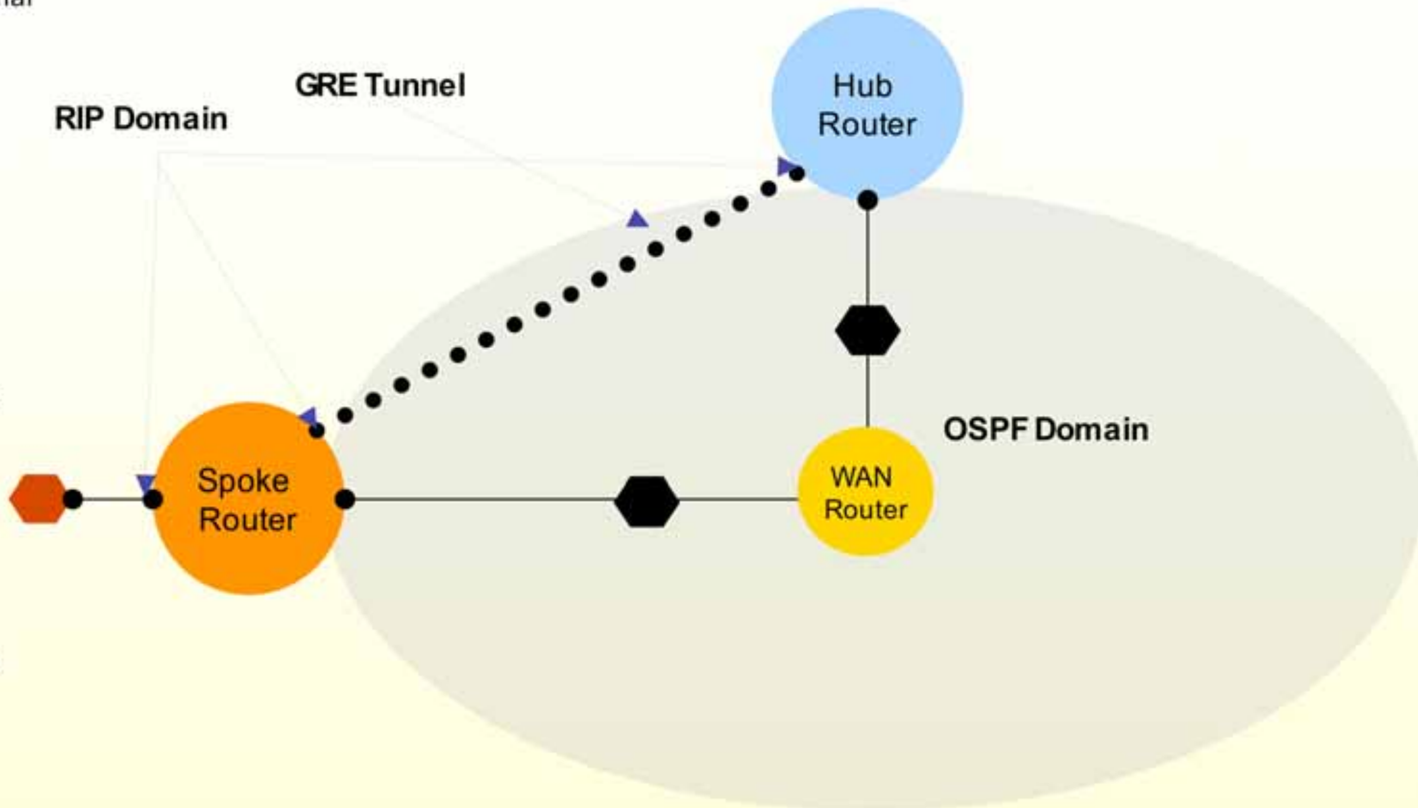
5. A router does not have more than one interface on a subnet
6. All internal interfaces are on internal subnets
7. All external interfaces are on external subnets
8. Every hub and spoke router is connected to a WAN router
9. No two non-WAN routers share a subnet

RoutingRequirements

10. RIP is enabled on all internal interfaces
11. OSPF is enabled on all external interfaces

GRERequirements

12. There is a GRE tunnel between each hub and spoke router
13. RIP is enabled on all GRE interfaces



To synthesize network, satisfy R1-R13 for
- previous list of components &
- 1 GRE tunnel

NOTE: GRE tunnel set up and RIP domain extended to include GRE interfaces automatically!

Strengthening Requirement: Adding Security For Overlay Network

RouterInterfaceRequirements

1. Each spoke router has internal and external interfaces
2. Each access server has internal and external interfaces
3. Each hub router has only external interfaces
4. Each WAN router has only external interfaces

SubnettingRequirements

5. A router does not have more than one interface on a subnet
6. All internal interfaces are on internal subnets
7. All external interfaces are on external subnets
8. Every hub and spoke router is connected to a WAN router
9. No two non-WAN routers share a subnet

RoutingRequirements

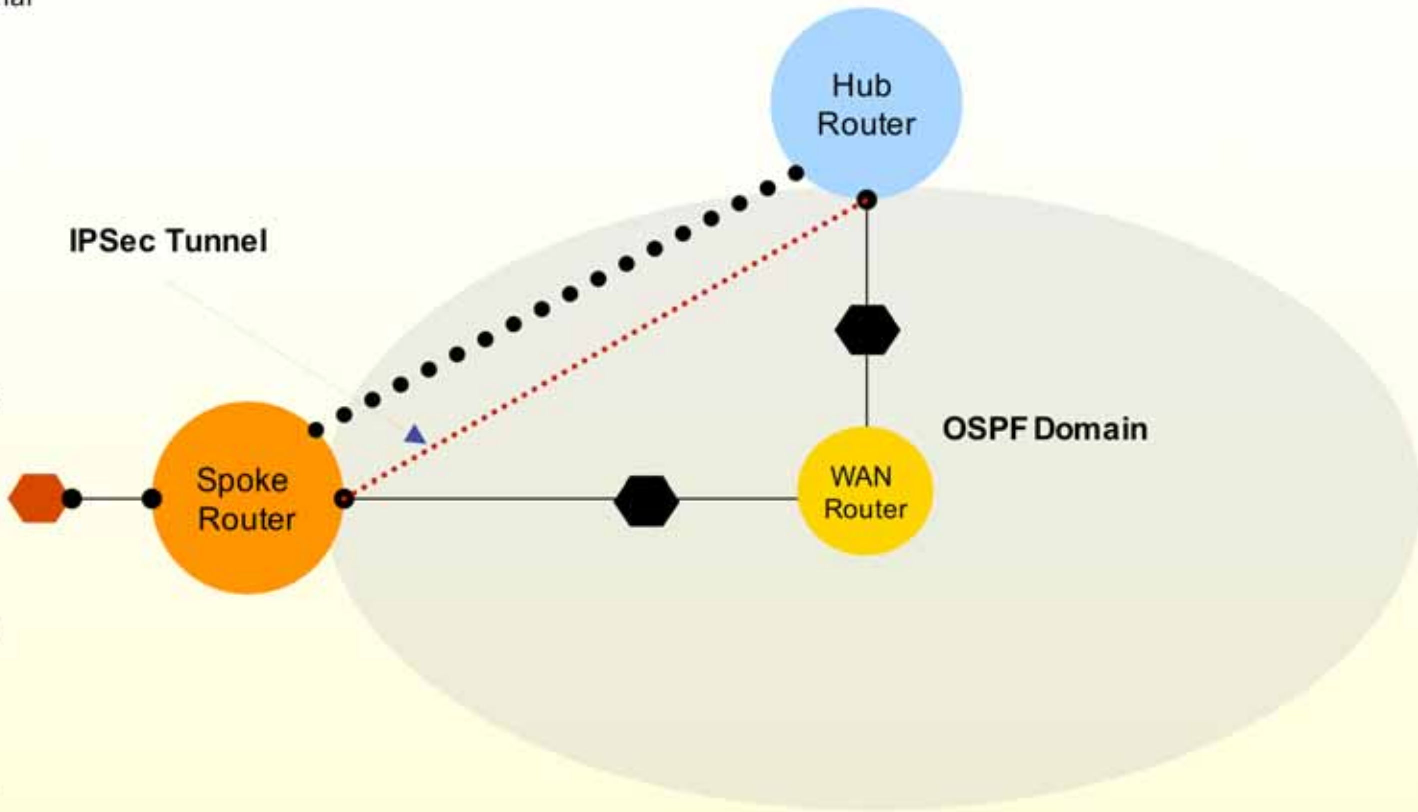
10. RIP is enabled on all internal interfaces
11. OSPF is enabled on all external interfaces

GRERequirements

12. There is a GRE tunnel between each hub and spoke router
13. RIP is enabled on all GRE interfaces

SecureGRERequirements

14. For every GRE tunnel there is an IPSec tunnel between associated physical interfaces that secures all GRE traffic



To synthesize network, satisfy R1-R14 for
- previous list of components &
- 1 IPSec tunnel

NOTE: IPSec tunnel securing GRE tunnel set up automatically

Strengthening Requirement: Adding Remote Access Service

RouterInterfaceRequirements

1. Each spoke router has internal and external interfaces
2. Each access server has internal and external interfaces
3. Each hub router has only external interfaces
4. Each WAN router has only external interfaces

SubnettingRequirements

5. **A router does not have more than** one interface on a subnet
6. All internal interfaces are on internal subnets
7. All external interfaces are on external subnets
8. Every hub and spoke router is connected to a WAN router
9. No two non-WAN routers share a subnet

RoutingRequirements

10. RIP is enabled on all internal interfaces
11. OSPF is enabled on all external interfaces

GRERequirements

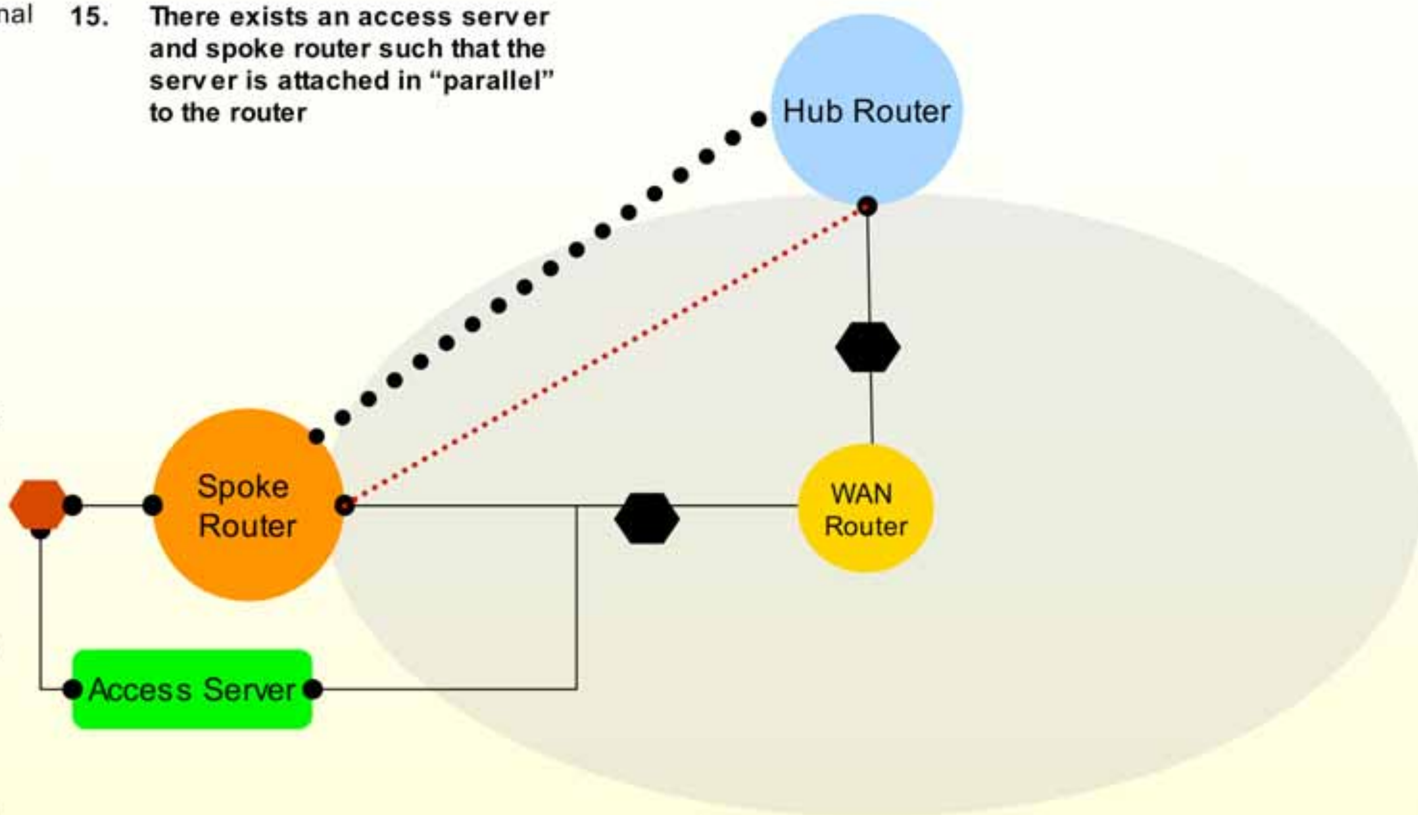
12. There is a GRE tunnel between each hub and spoke router
13. RIP is enabled on all GRE interfaces

SecureGRERequirements

14. For every GRE tunnel there is an IPSec tunnel between associated physical interfaces that secures all GRE traffic

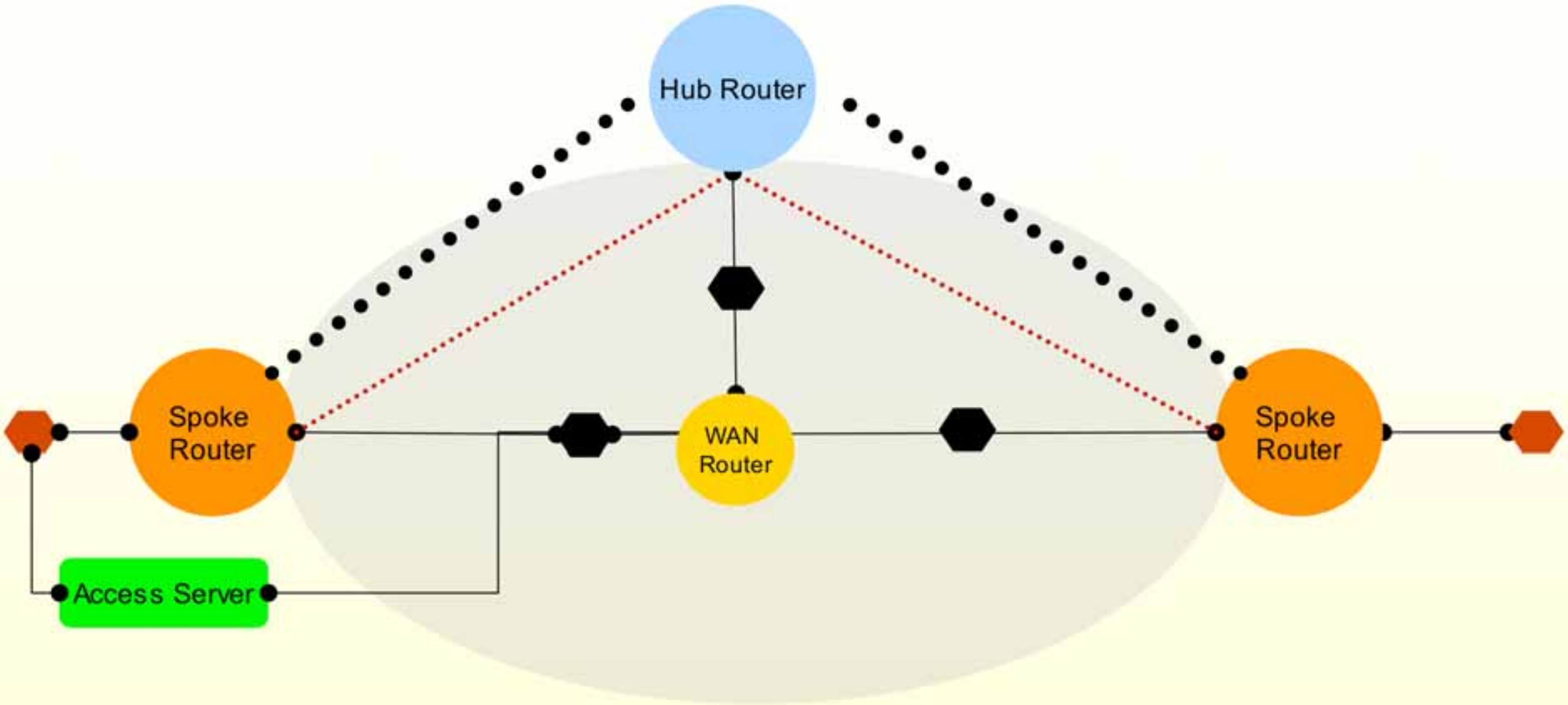
AccessServerRequirements

15. **There exists an access server and spoke router such that the server is attached in "parallel" to the router**



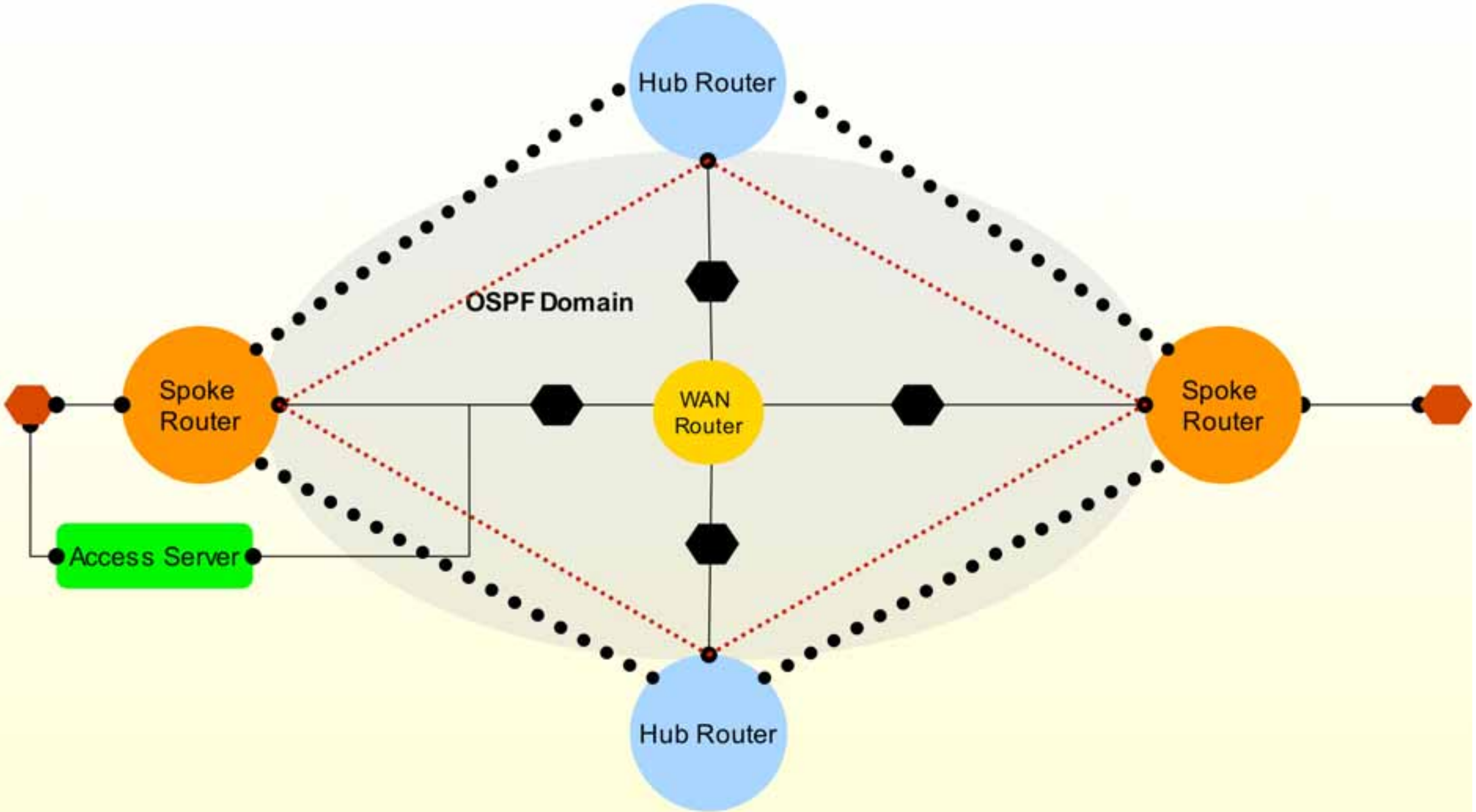
- To synthesize network, satisfy R1-R15 for previous list of components and 1 additional access server.
- Note: Access server interfaces placed on correct interfaces and RIP and OSPF domains correctly extended with internal and external interfaces, respectively

Component Addition: Adding New Spoke Router



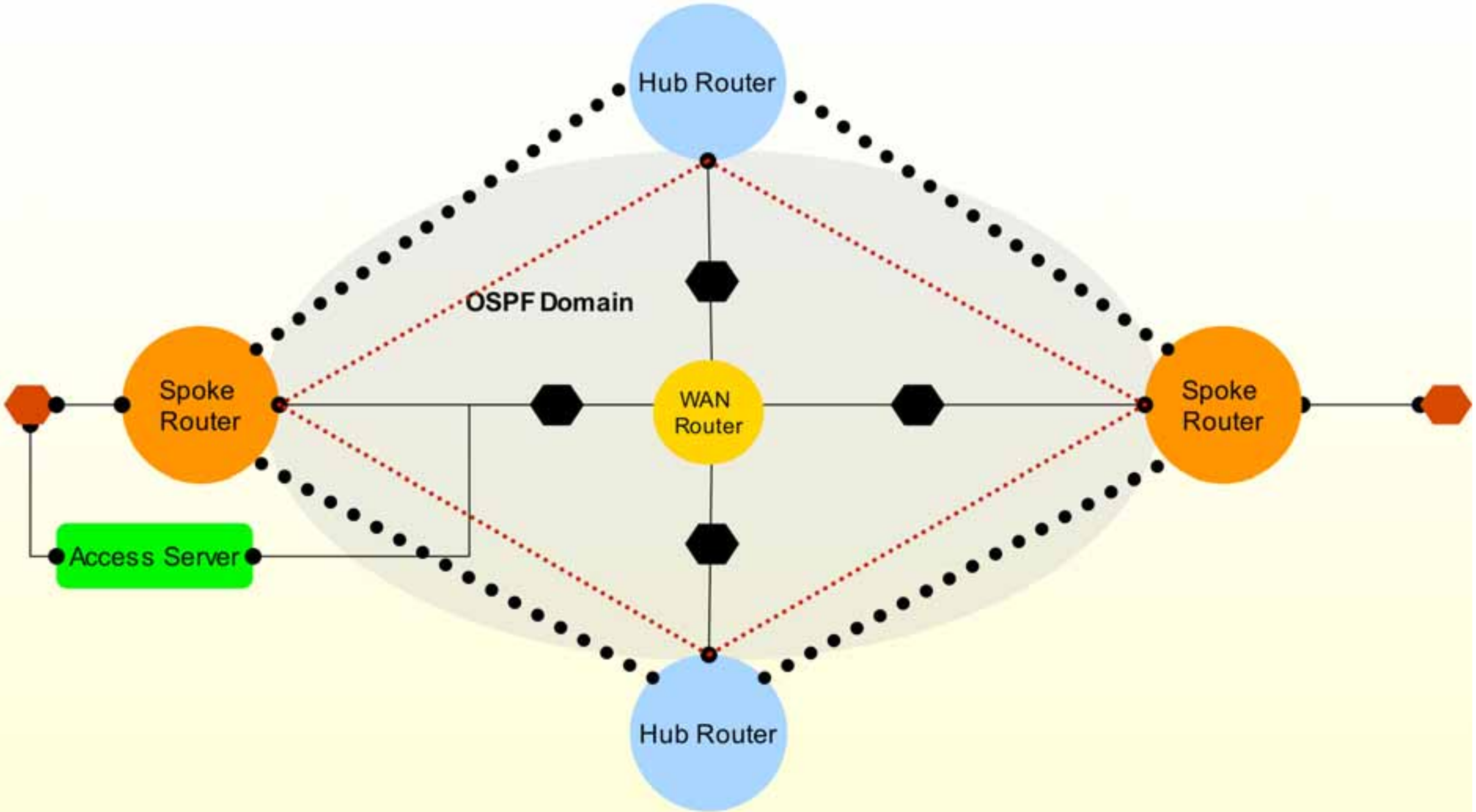
- To add another spoke router satisfy requirements R1-R16 for previous components and one additional spoke router and related components
- Note: New subnets, GRE and IPSec tunnels set up, and routing domains extended *automatically*

Component Addition: Adding New Hub Router



- To add another hub router satisfy requirements R1-R16 for previous components and one additional hub router (and related com[ponents)
- New subnets, GRE and IPSec tunnels set up, and routing domains extended *automatically*

Verification: Adding Firewall Requirements & Discovering Design Flaw



- Symptom: Cannot ping from one internal interface to another
- Define Bad = ip packet is blocked
- Check if R1-R16 & Bad is satisfiable
- Answer: WAN router firewalls block ike/ipsec traffic
- Action: Create new policy that allows WAN router firewalls to pass esp/ike packets

Summary & Future Directions

- Configuration plays central role in web services infrastructure synthesis & management
- We need a theory of configuration to automate synthesis and realize "autonomic" behavior
- Fundamental problems:
  1. Specification languages
  2. Configuration synthesis
  3. Incremental configuration (requirement strengthening, component addition)
  4. Configuration error diagnosis
  5. Configuration error troubleshooting
  6. Verification
  7. Configuration sequencing
  8. Distributed configuration
- Proposed formalization of 1-7 via Alloy and SAT solvers
- Future directions:
  - Scalable *algorithms* to solve above problems.

Thank You