

Mitigation Strategies

Based on SROC class given by Hervey Allen, Chris Evans, and Phil Regnaud 2009 Santiago, Chile





Overview

- Where Did We Start?
- Where We are Now...
- Survey of Additional Strategies

Where Did We Start?

- We started with a fairly simple, non-resilient network
 - One Nameserver
 - One Non-Functional NOC

We Were “Blind”!

We Are Here!

- We now have a fairly simple network that offers us some resiliency to cyber attacks
 - One Nameserver
 - Some Configuration Changes
 - One Functional NOC
 - Monitoring & Detection

We Can See!

We Are Here!

- The Things We Discussed:
 - Have a Plan BEFORE Attacks Occur
 - Various Monitoring Tools
 - Configuration Control
 - Secure Application Configurations
 - Segregated Machines and Networks

Tip of the Iceberg!

It's a BIG World...

- There are things that we didn't demonstrate due to time or have the ability to add:
 - Anycasting
 - Additional Infrastructure
 - In-Line Monitoring
 - Active Defenses

But – Let's Discuss!

"By The Way – Not Everything Is a Technical Solution!"

Mitigation Strategies

- Build a Contingency Plan
 - Compare costs of disruption vs. recovery
 - Establish plan of action for what you expect to be your highest risks
 - Concentrate on your business objectives & risk
 - Risk is NOT threat – its an understanding of what's important to you, threats, vulnerabilities, controls, and impact
 - Prioritize security implementations based on risk
 - You probably don't have the time or resources to implement everything
- Good security is about multiple layers of protection



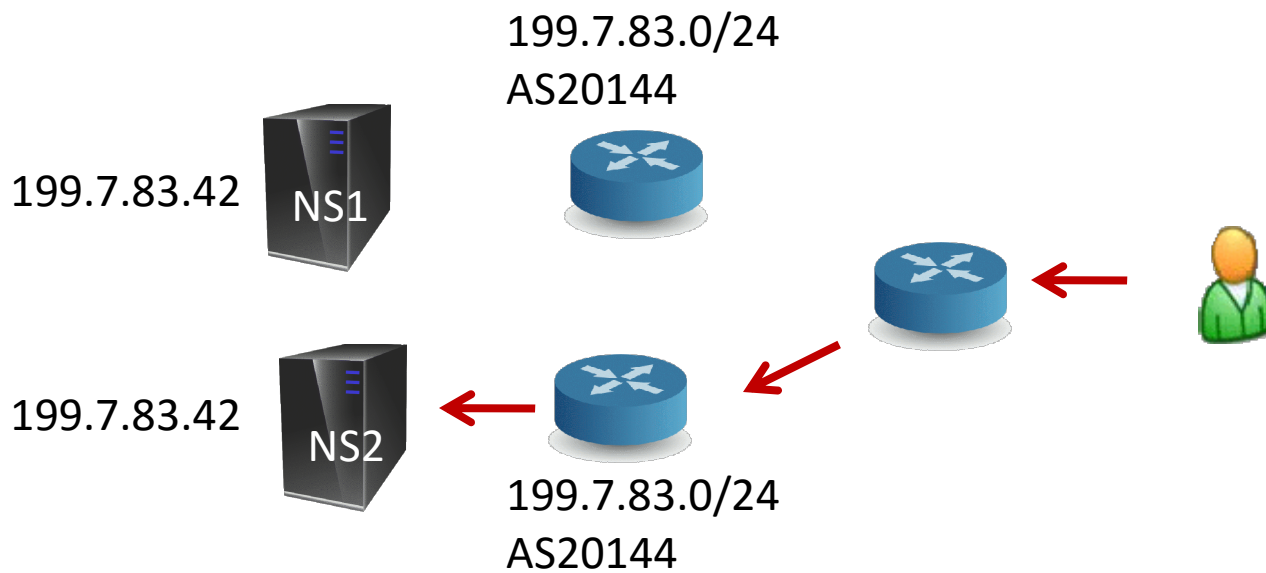
Mitigation Strategies

- Robust Architectures
 - Anycasting
 - Geographically Separated Name Servers
 - NS on Both Sides of Satellite Links
 - Diversity in hardware & software
 - Over-provision where possible
 - Bandwidth, servers, people!

Mitigation Strategies

- Anycasting

“Anycast is a network addressing and routing scheme whereby data is routed to the "nearest" or "best" destination as viewed by the routing topology.” – *Wikipedia*



Mitigation Strategies

- Anycasting
 - Increased Capacity, Resiliency to Attack
 - Outsourcing
 - Instant Gratification, Perhaps Loss of Control
 - What are you really getting? Ask Questions!
 - Doing it In House
 - Requires Expertise & Resources to Set it Up

Mitigation Strategies

- Real Time Monitoring
 - Stratify your alerts (info, low, med, high, uh oh!)
 - E-Mail, SMS, Pager notifications of priority alerts
 - Select tools that work for you!
- Intrusion Detection
 - Install & Monitor an IDS (e.g. SNORT)
 - Where to install it? Inside or Outside?
 - Feeling adventurous – put it in active mode!

Mitigation Strategies

- Vulnerability Scanning
 - Regularly scheduled scans – using an updated engine!
 - Web application, operating system, third party application scanners are all available...
- Patching Systems
 - This is NOT a silver bullet – but keeps riff-raff out
 - Use automatic updates where available
 - Vulnerability scanning can tell you what's missing – don't assume that because you "installed" it, it actually took
 - Don't forget 3rd party application updates (adobe, flash, firefox, etc)



Mitigation Strategies

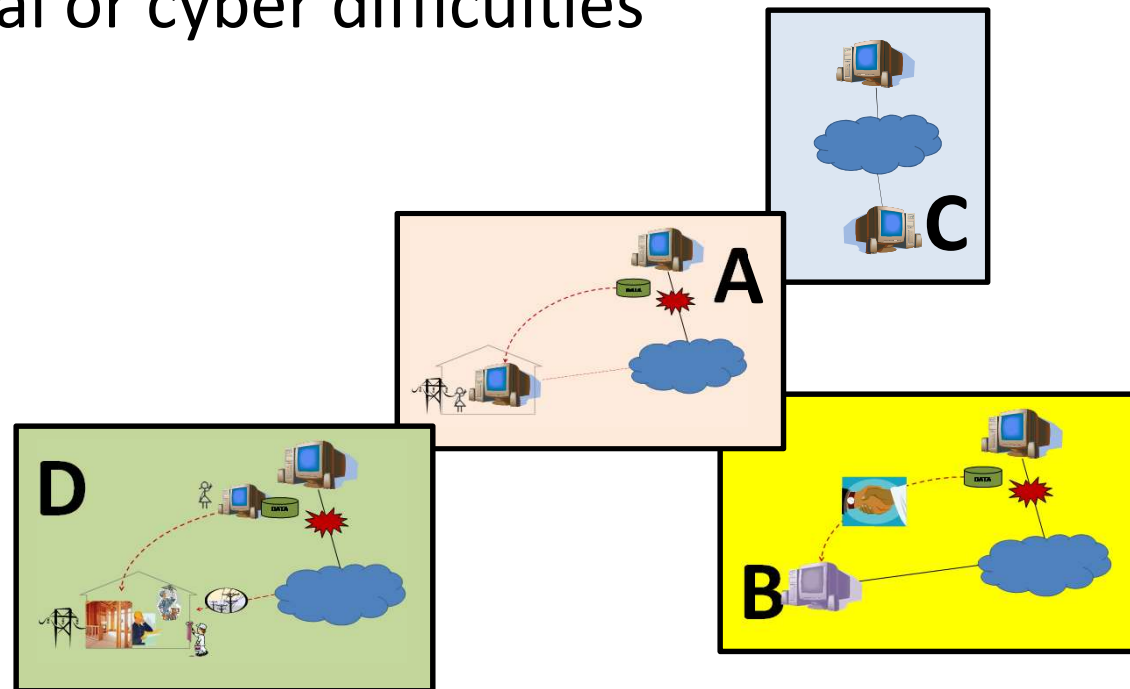
- Forensic Data Capture
 - Capture the last say, 12 hours, of traffic to enable you to do forensic analysis on what happened after the fact
- Technical Configuration Guides
 - Understand how your systems are configured and be able to easily reproduce / rebuild them
 - Most already exist, find them BEFORE you need them in a hurry

Mitigation Strategies

- Data Escrow
 - Keeping a copy of your zone and customer data in a safe place
- Mutual Aid Agreements
 - Other ccTLDs, Universities, Governments
 - Secondary Hosts, Data Escrow, Tech Assistance
 - Temporary Manpower & Resources
 - Do you (would you) share data of an attack with other ccTLDs?

Mitigation Strategies

- Cold, Warm, Hot & Mirrored Sites
 - Secondary locations that can be stood up in case of physical or cyber difficulties



Mitigation Strategies

- Bubba Net (Bubba = Friend, Net = Network)
 - Establish your professional networks so you know who to call when you need assistance
- Develop Professional Network of Stakeholders
 - Governments, ISPs, Registrars, etc
- Awareness Briefings to Stakeholders
 - Establish yourself as “critical infrastructure”



Mitigation Strategies

- End User / Customer Education
 - Reduce Risk from Your Customers (e.g. phishing)
- Media / Public Relations
 - Invite media in to discuss best methods of dealing with them
 - Build a communication plan so you know how to respond for a given situation



Mitigation Strategies

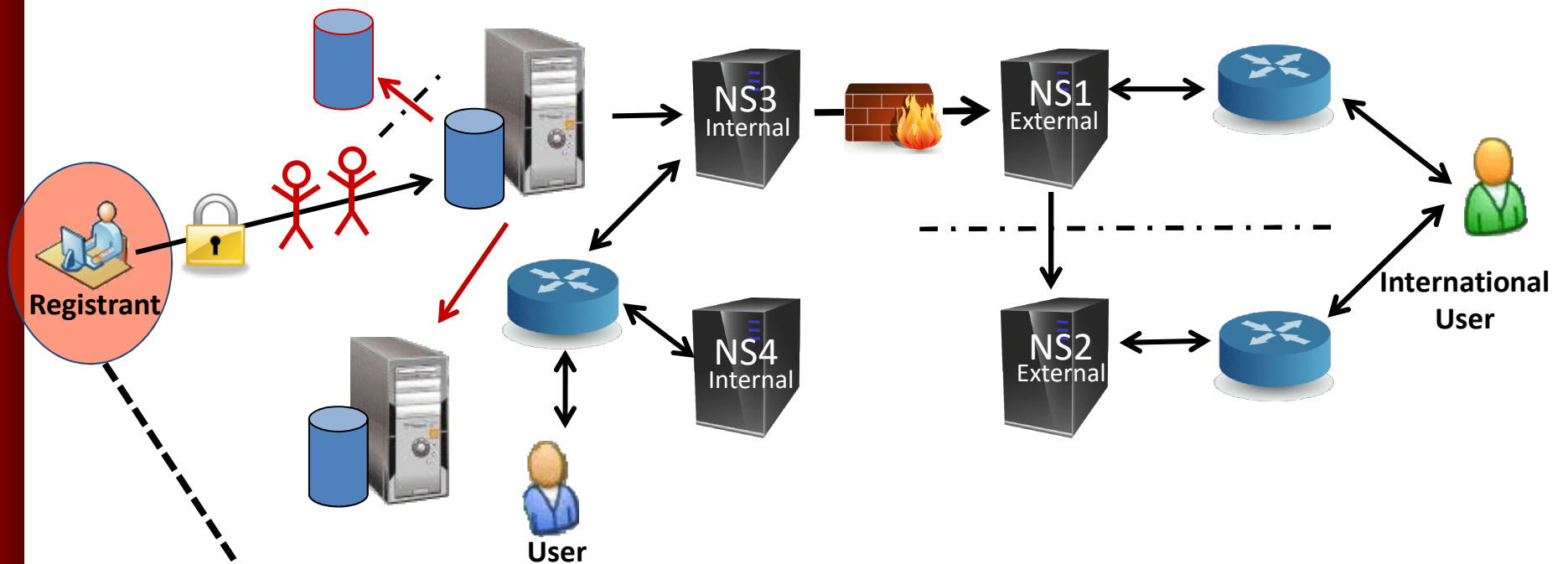
- Internal Training & Awareness
 - Train your administrators in defensive actions
 - Forces you to establish procedures & policies!
- Exercise Defensive Actions
 - You will only know your defensive capacity by testing it!
 - Simple walkthroughs to elaborate, hands-on, multi-agency exercises



Mitigation Strategies

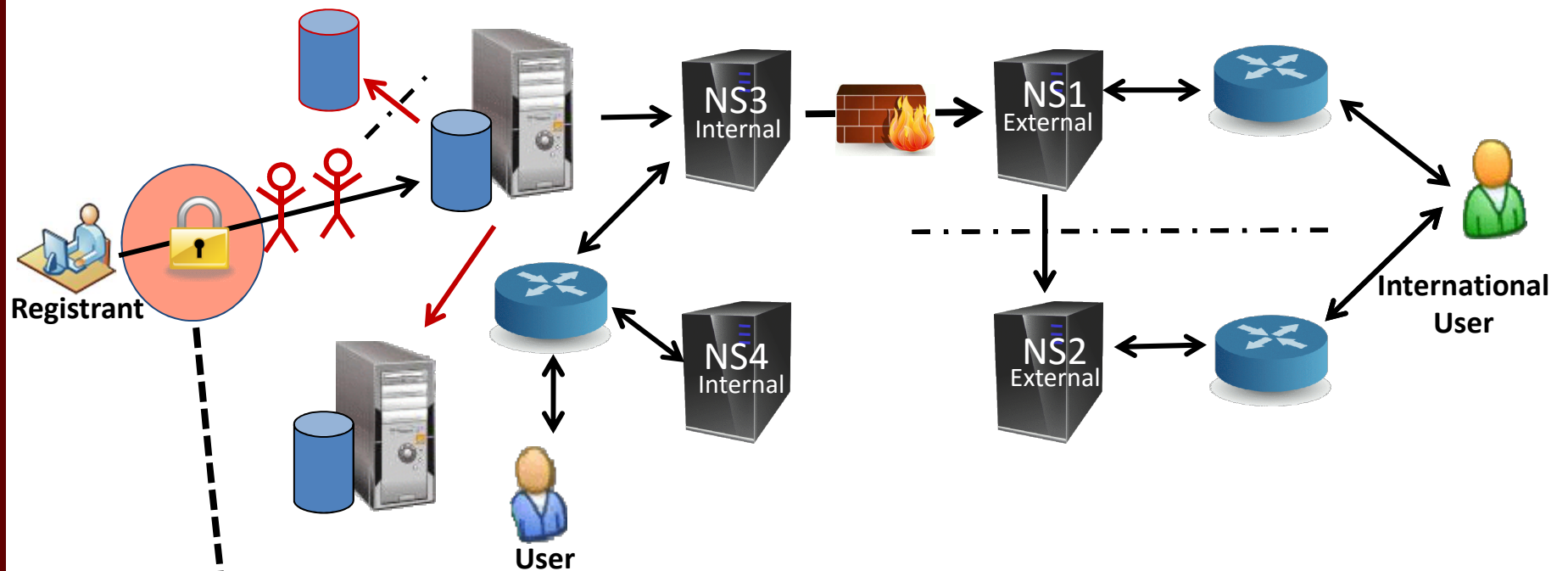
- Test Your Processes
 - Two-factor authentication for customer interaction
 - Out of band communication (phone, fax, walk-in) for customer validation

Notional ccTLD Architecture



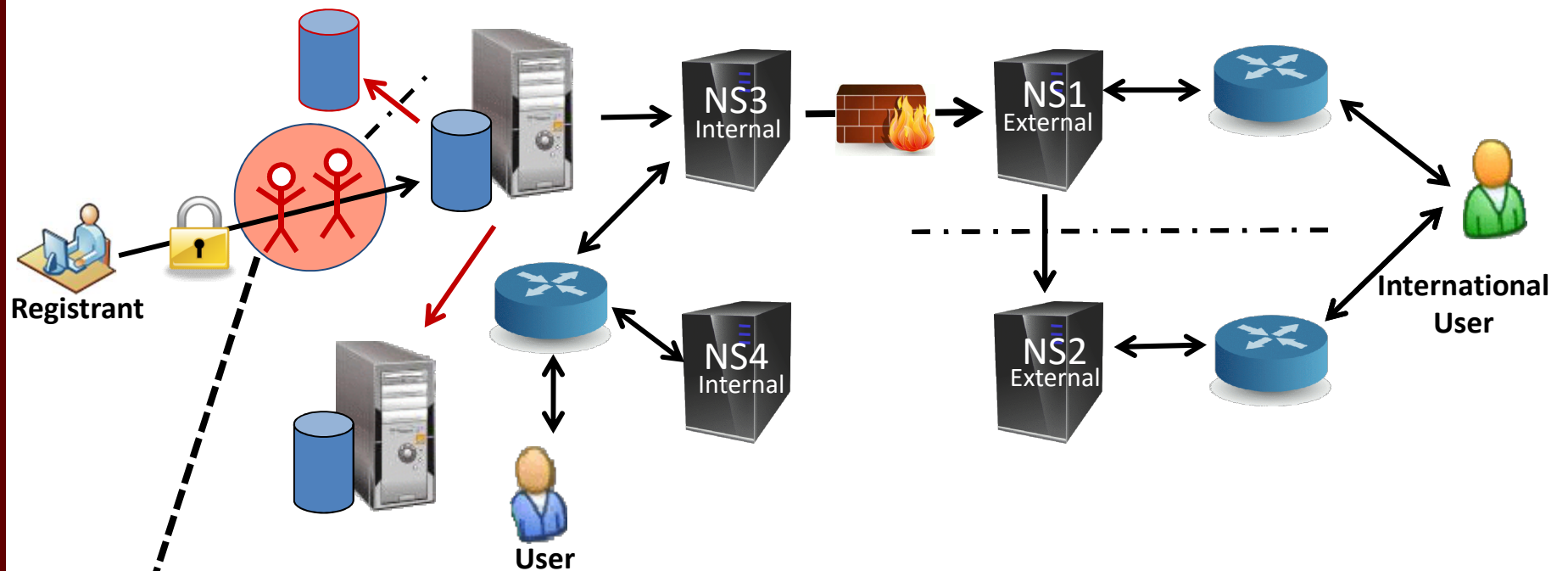
Registrant – Requests Assignment, Updates, Removal

Notional ccTLD Architecture



Authentication for Registrant Requests

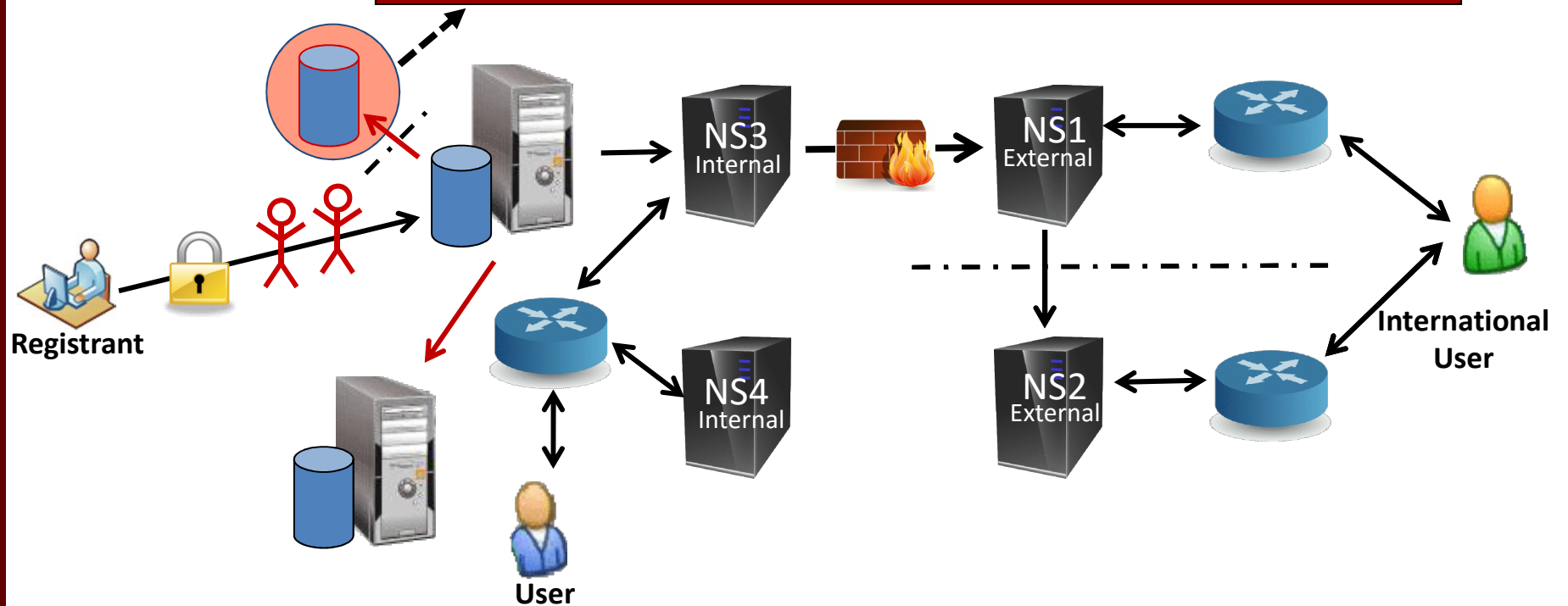
Notional ccTLD Architecture



Authorization for Internal Registry Changes

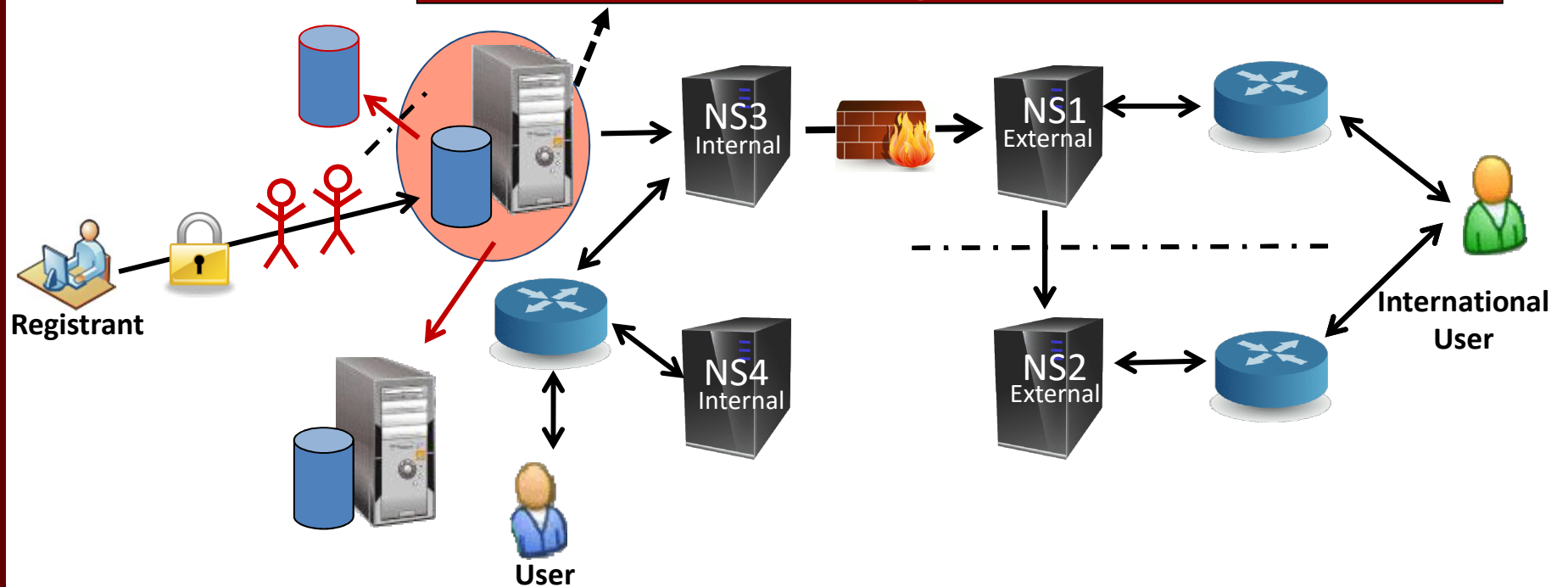
Notional ccTLD Architecture

Offsite Backup for Entire Registry

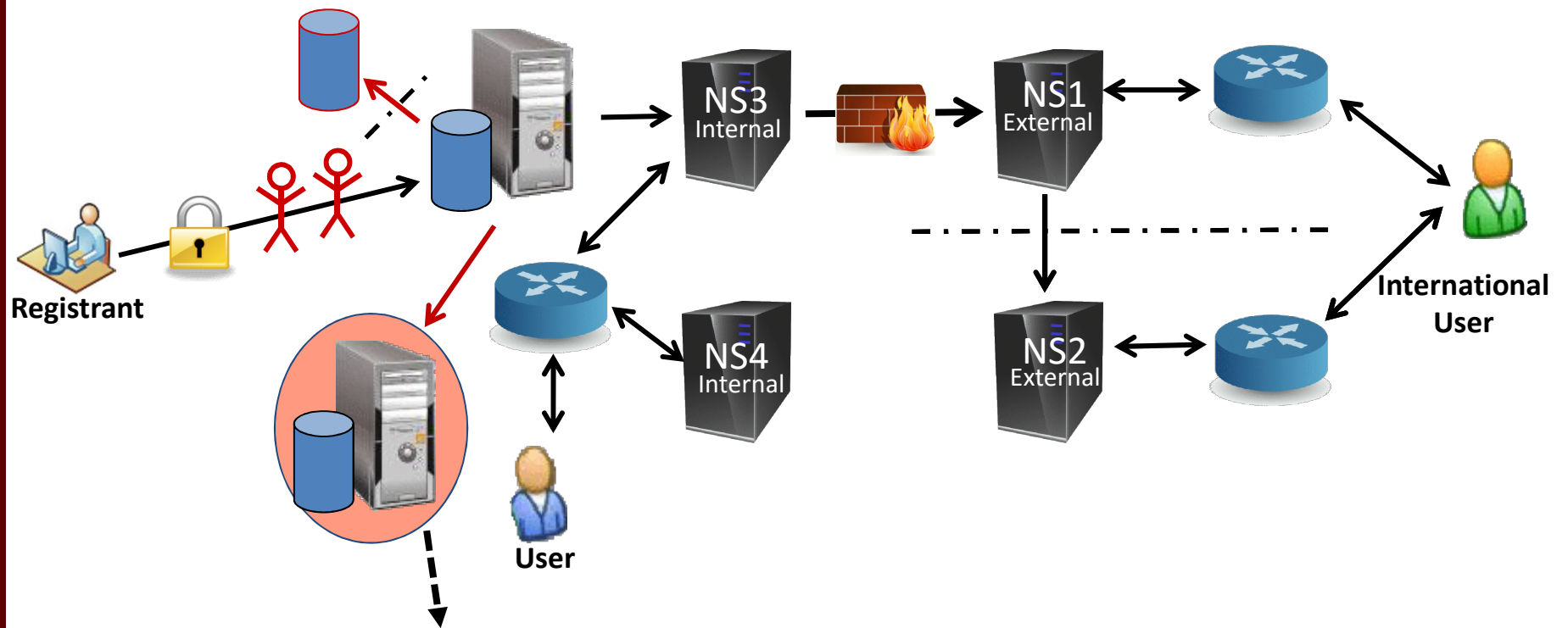


Notional ccTLD Architecture

Registry – Publishes and Maintains Assignments

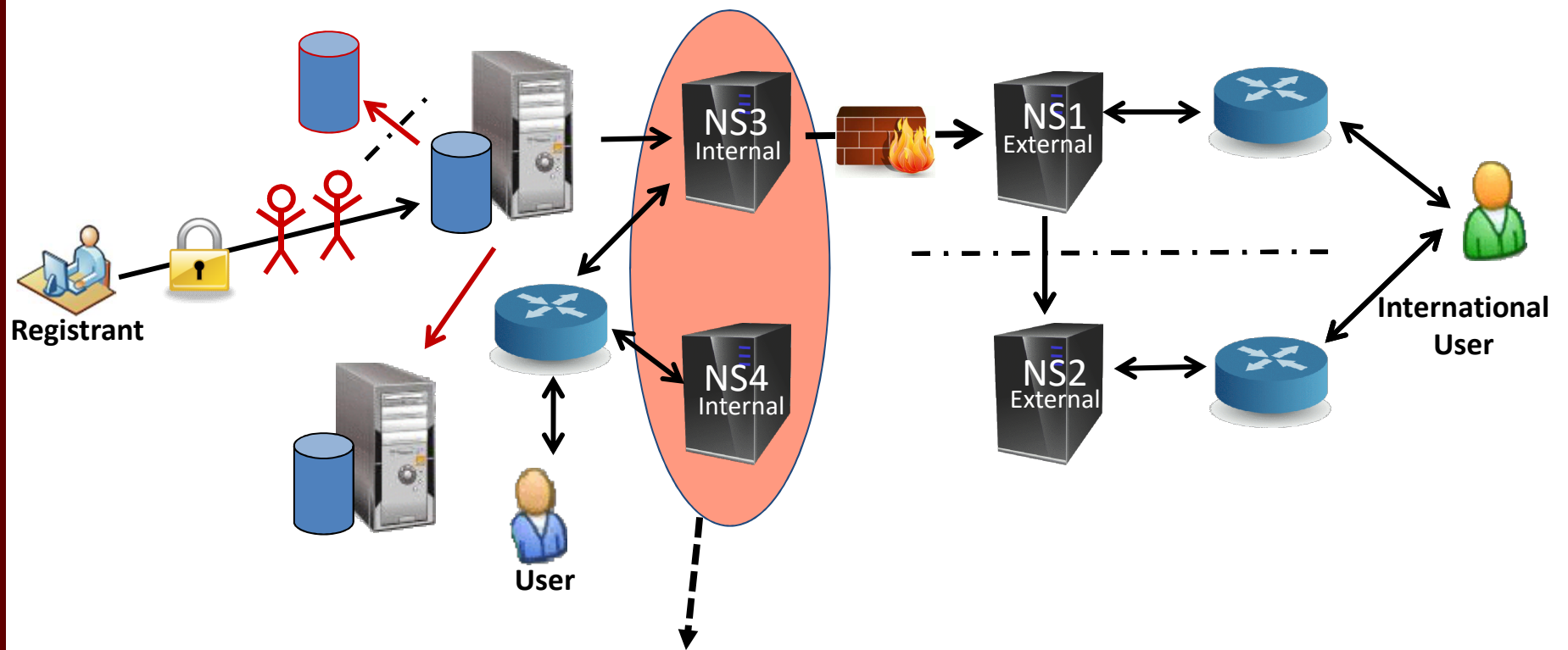


Notional ccTLD Architecture



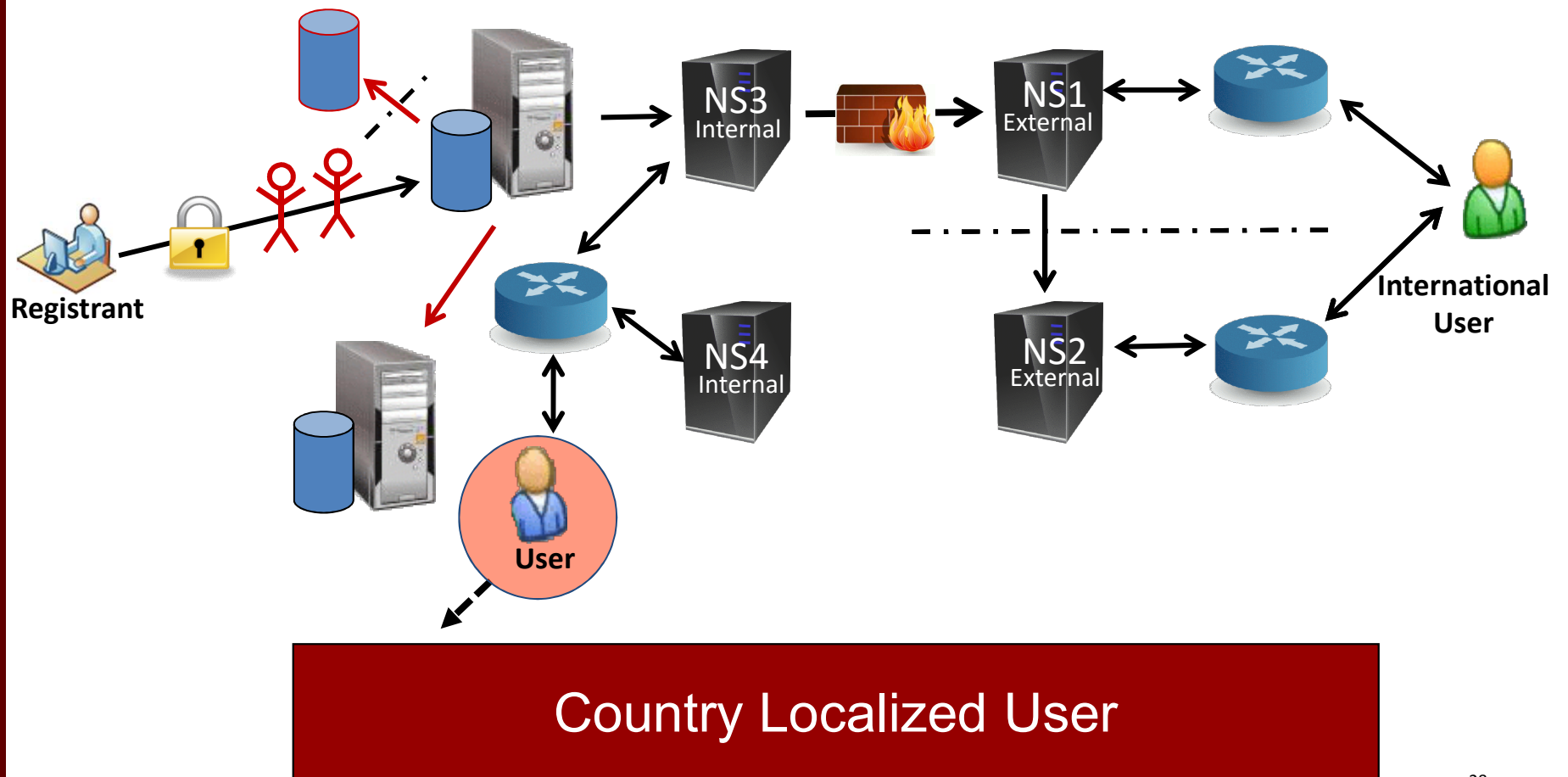
Alternate Registry Server and Database

Notional ccTLD Architecture

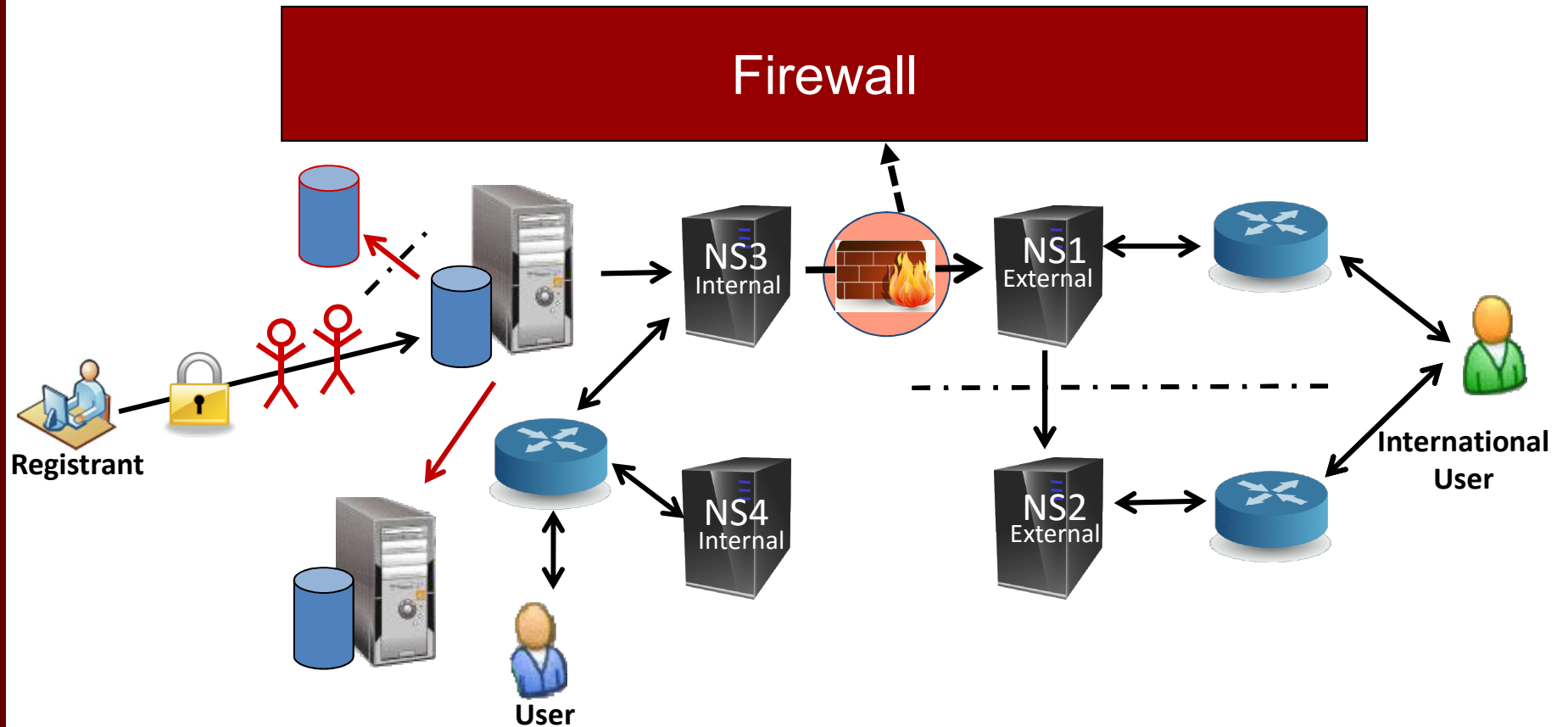


Country Localized DNS Servers

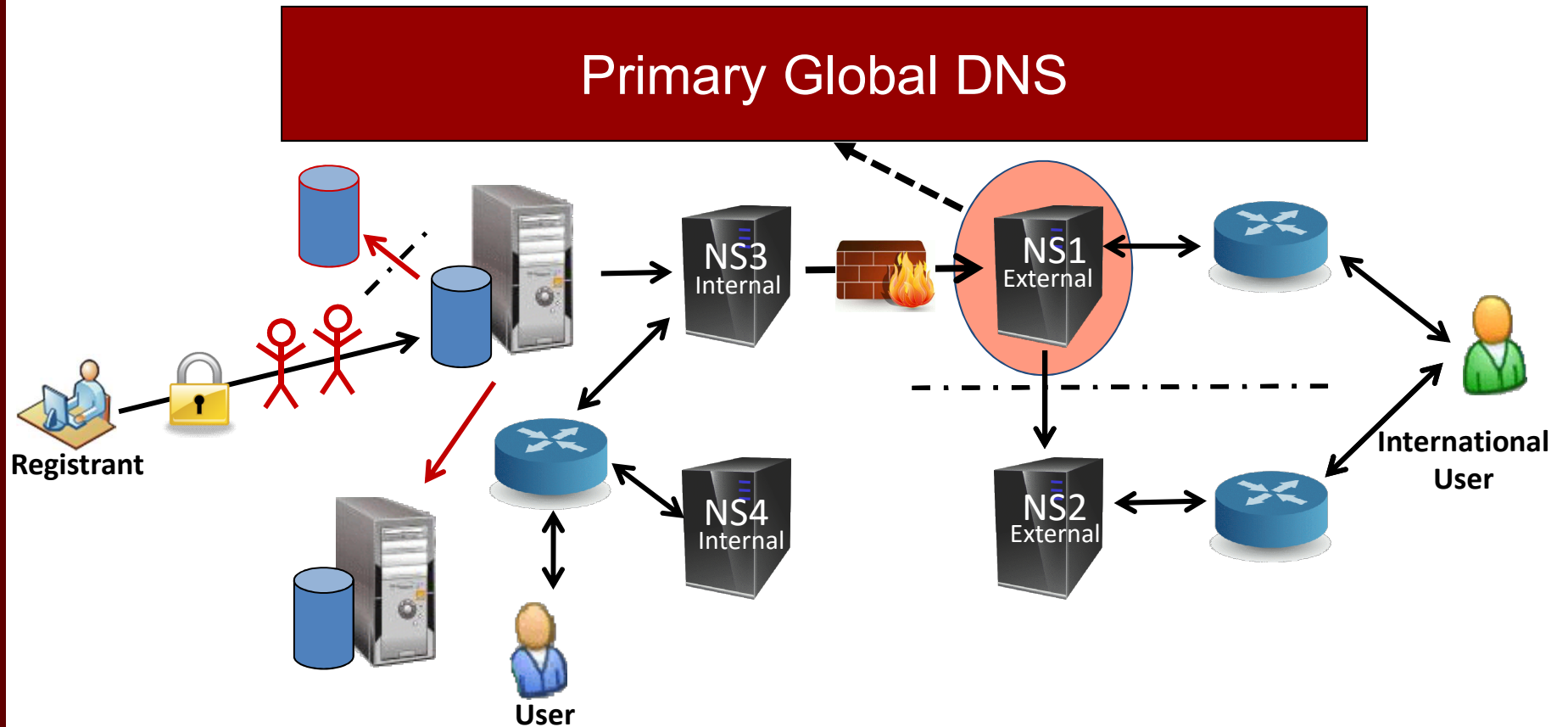
Notional ccTLD Architecture



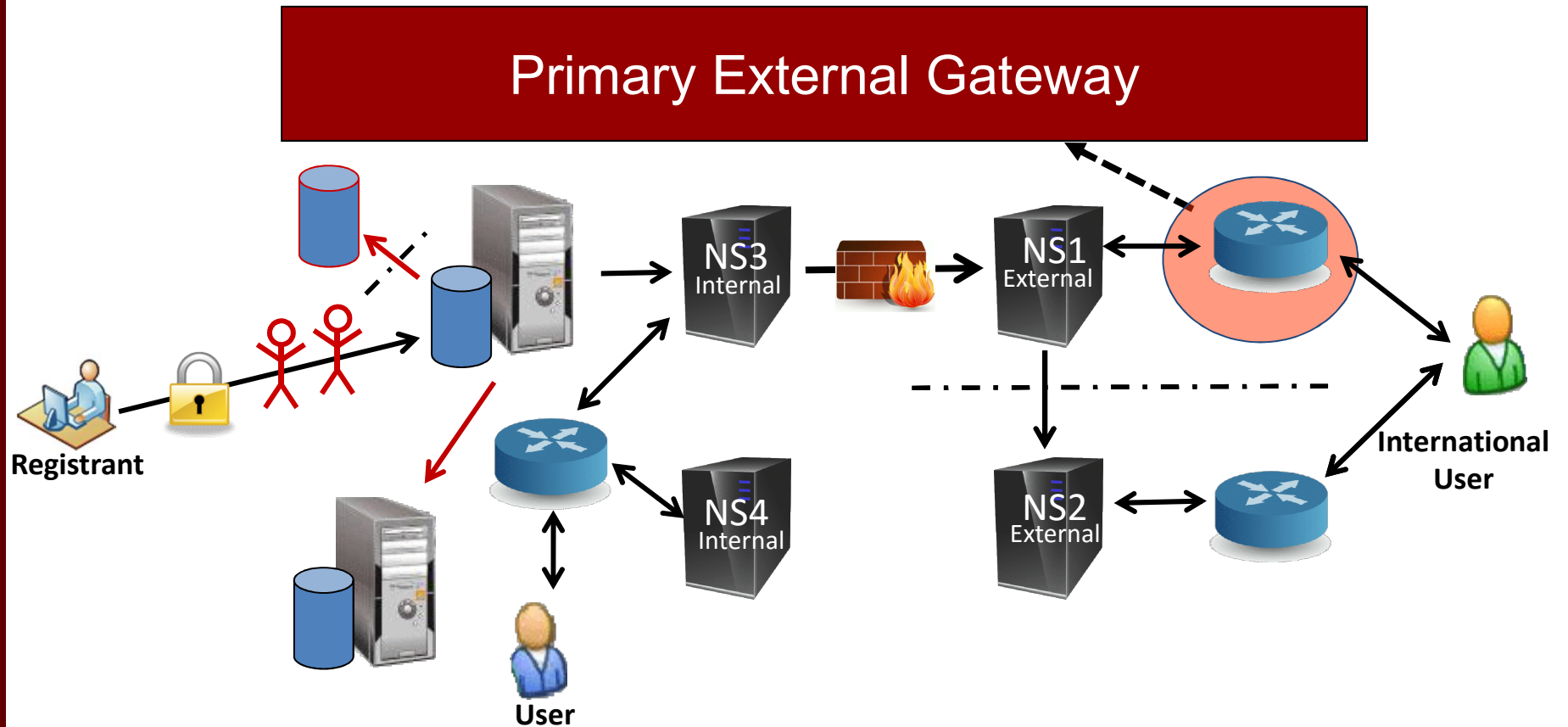
Notional ccTLD Architecture



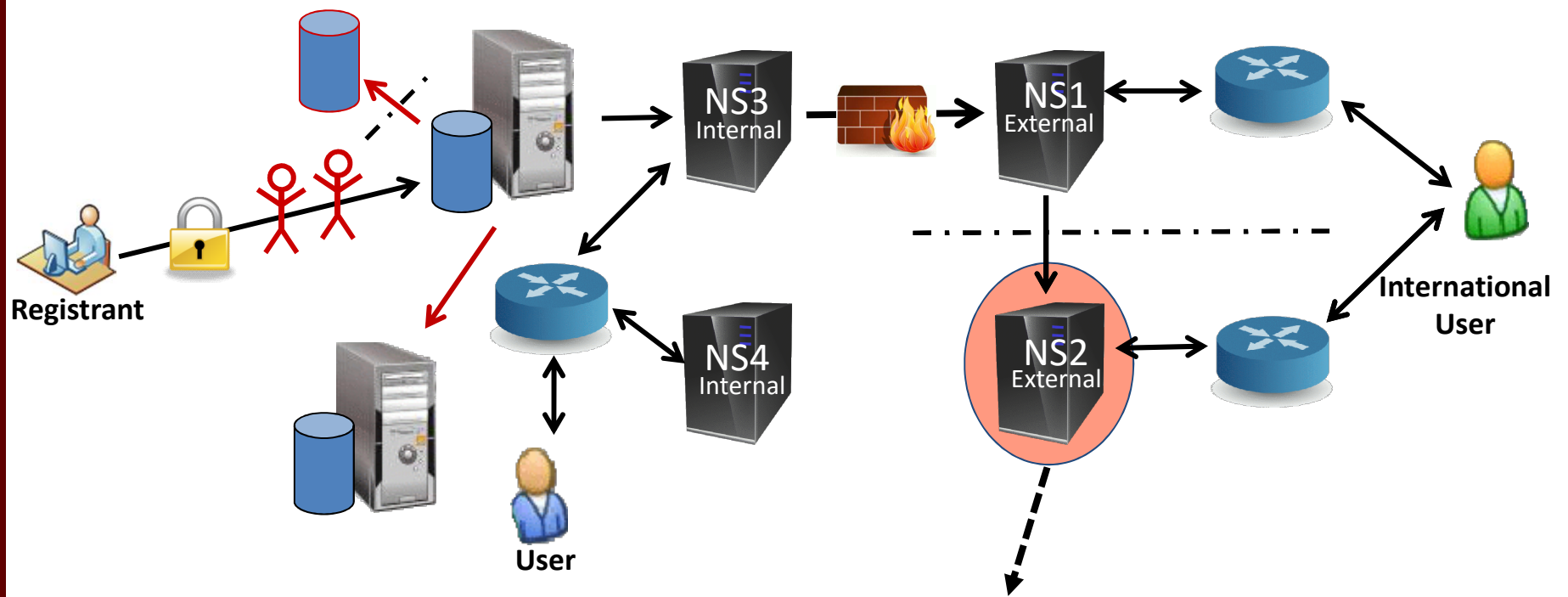
Notional ccTLD Architecture



Notional ccTLD Architecture

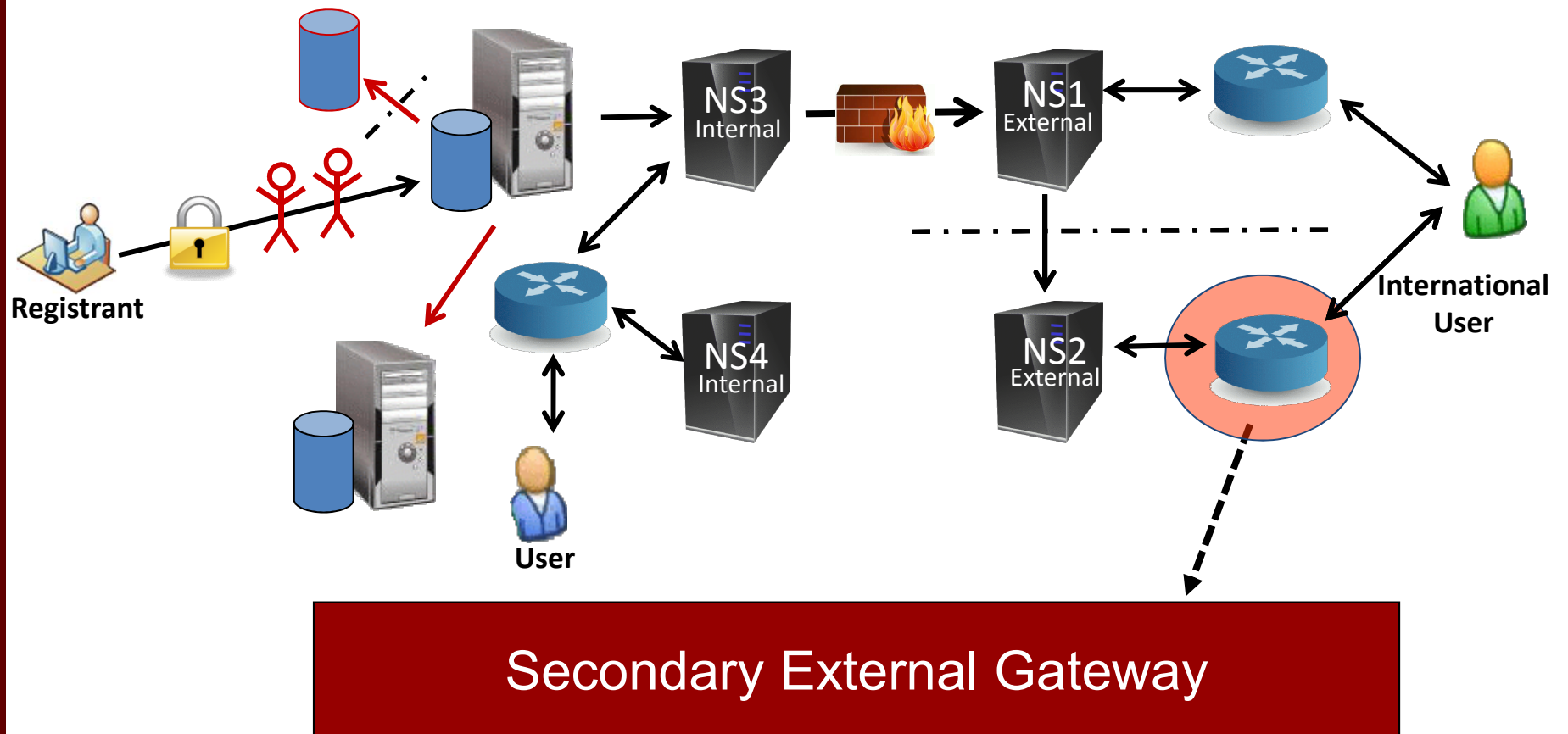


Notional ccTLD Architecture

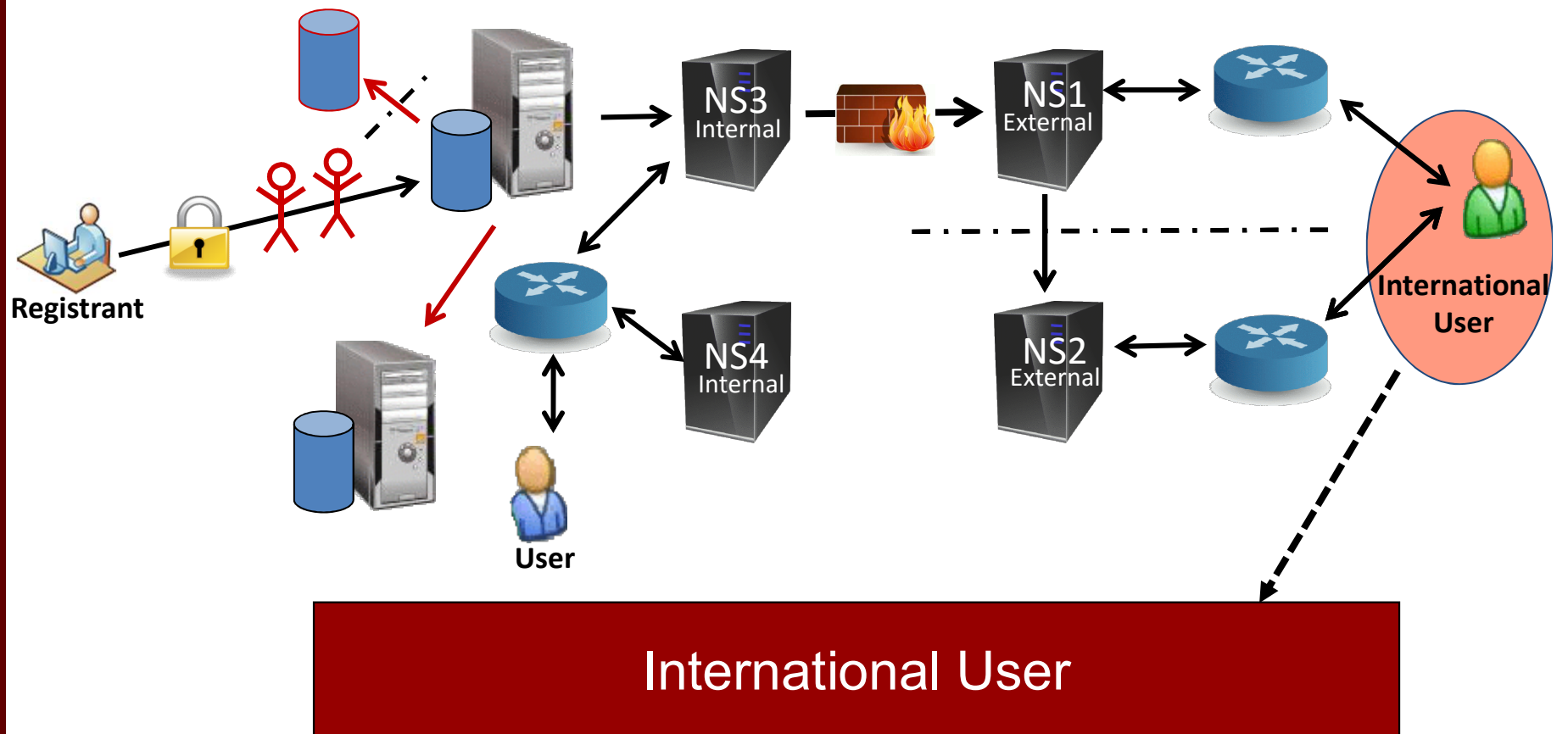


Secondary Global DNS Server
Anycasting with Geographic Separation

Notional ccTLD Architecture



Notional ccTLD Architecture




Recommendations

Threat	Recommendations
Zone Transfer	Monitoring, DNS Server Configuration
Non-Authoritative Spoofing	Monitoring, Communication
Port Scanning	Monitoring, Awareness of Other Parallel Attacks
Router Re-Config	Monitoring, Configuration Control, Administrative VLANs
SSH Brute Force	Application Logging, Log Analysis, Secure Configuration
DDoS	Geographic Separation, Anycasting, Country Localized and Global Server Separation

References

- Internet Society Workshop Resource Center
<http://www.ccnog.org/>
- ccTLD Best Practices
<http://www.nsrc.org/netadmin/wenzel-cctld-bcp-02.html>
- ICANN Country Code Name Support Org
<http://ccnso.icann.org/>
- ICANN Security & Stability Advisory Committee
<http://www.icann.org/committees/security/>
- DNS Security Reading Room
<http://www.dnssec.net/dns-threats>



DNS Installation &
Configuration

QUESTIONS?

- Do you have any questions about ...
 - Mitigation Strategies

