

**SCOLD:**  
**Secure Collective Internet Defense**  
**A NISSC supported project**

**C. Edward Chow**

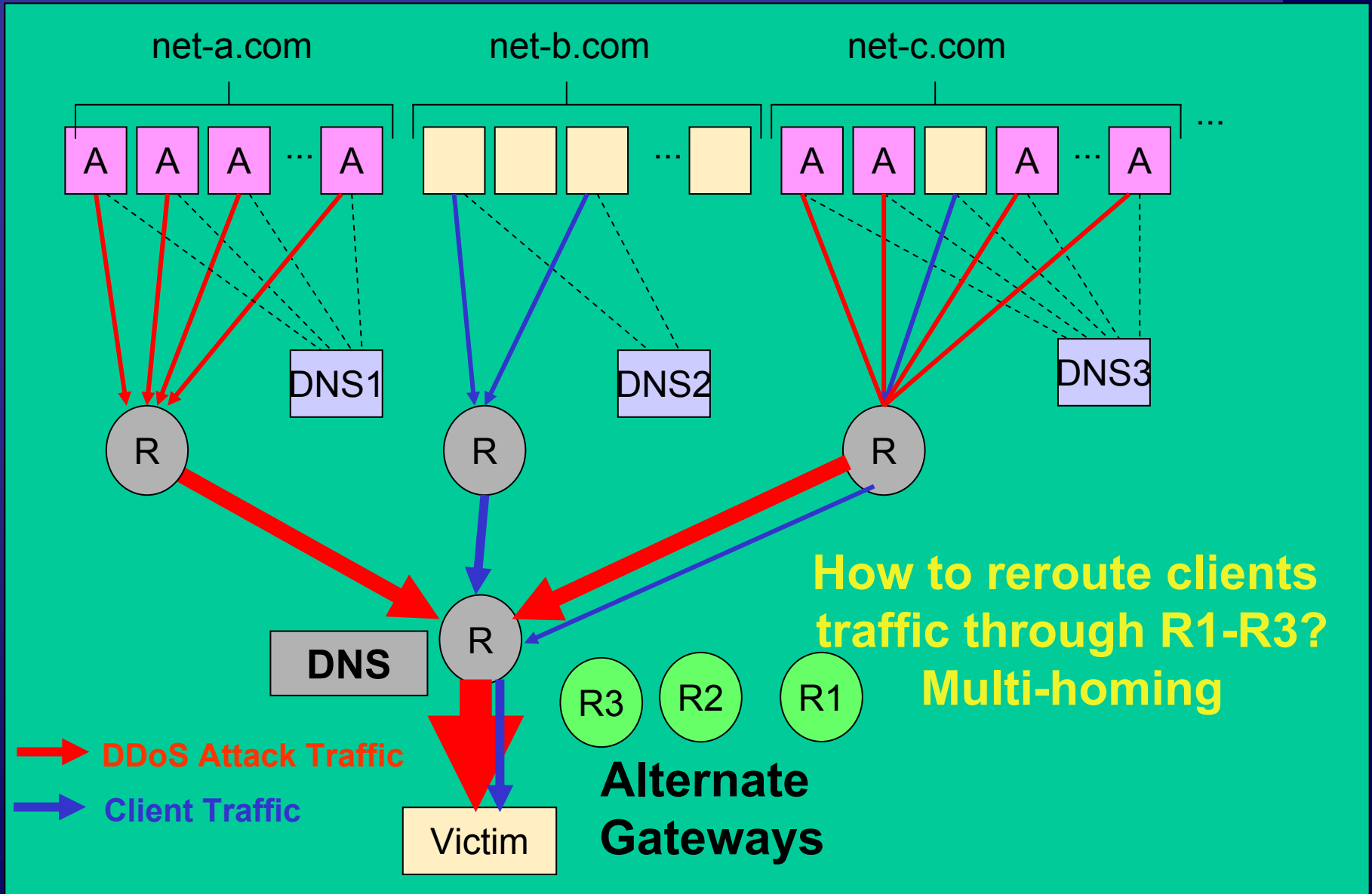
**Yu Cai**

**David Wilkinson**

**Sarah Jelinek**

Part of this work is based on research sponsored by the Air Force Research Laboratory, under agreement number F49620-03-1-0207. It was sponsored by a NISSC Summer 2003 grant.

# Wouldn't it be Nice to Have Alternate Routes?

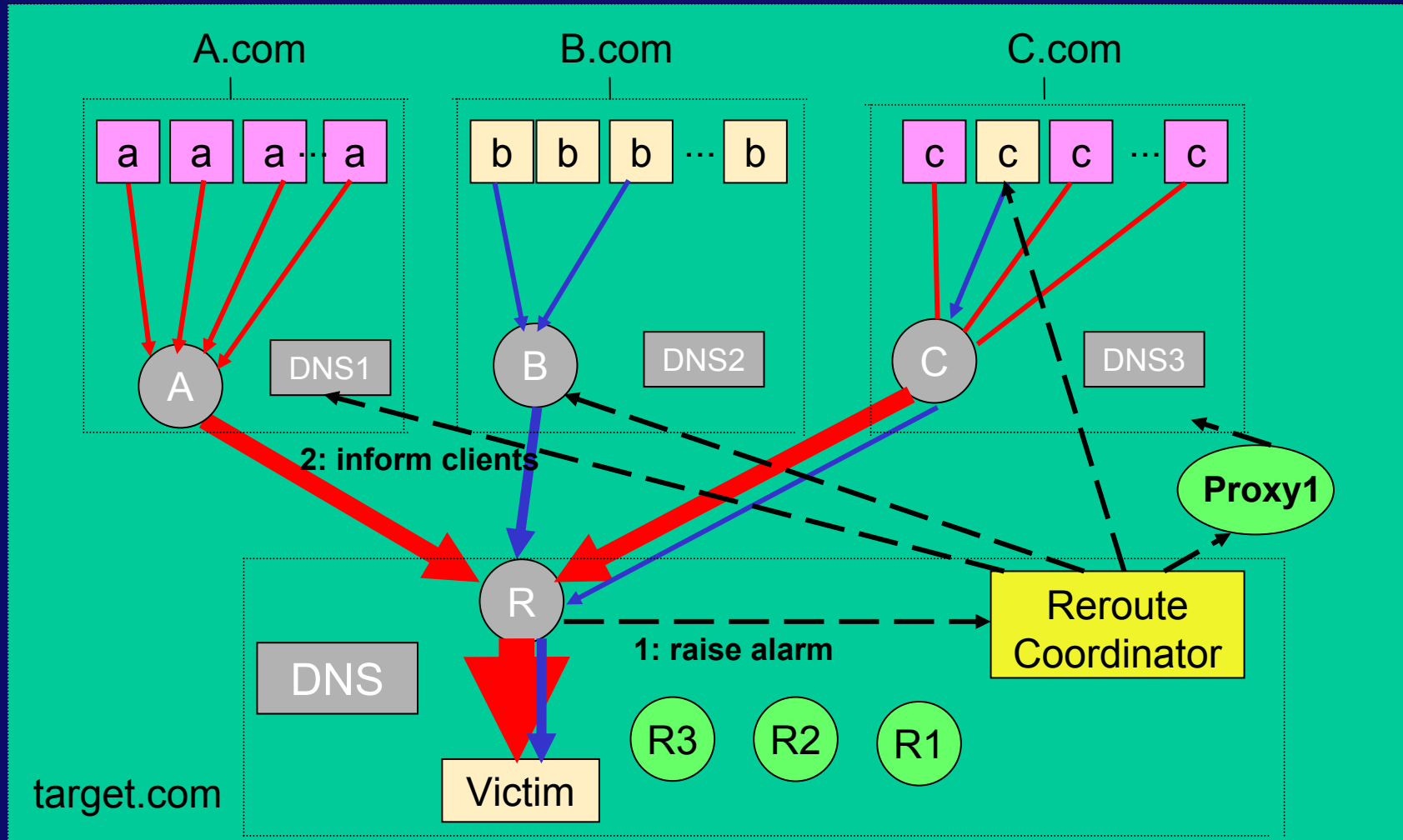


# Secure Collective Defense

- SCOLD main ideas:
  - Explore secure alternate paths for clients to come in by utilizing geographically separated proxy servers;
  - push back attack traffic by utilizing Intrusion Detection Isolation Protocol (IDIP).
- SCOLD techniques:
  - Utilize a consortium of Proxy servers with IDS to set up indirect route.
  - Clients use the new reroute information and route traffic through proxy servers.  
→ Use Sock protocol, modify resolver library
  - Secure DNS Update: inform client DNS servers to add new entries with a set of proxy servers IP addresses.
  - Push back using Intrusion Detection Isolation Protocol (IDIP).
  - Partition clients to come at different proxy servers, proxy server selection algorithms.
  - Proxy Server based Multipath Connections (PSMC)

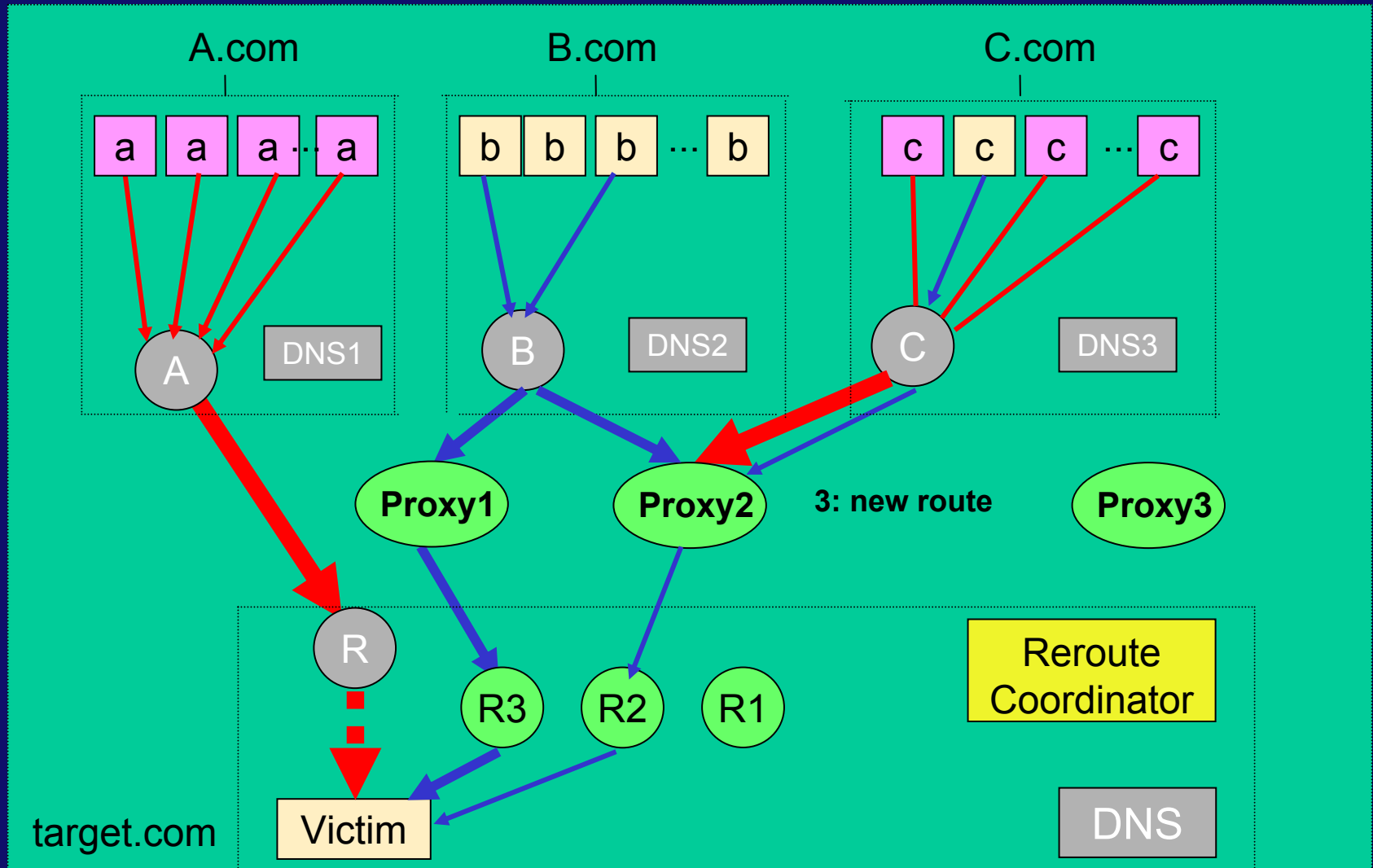


# SCOLD: raise alarm (1) and inform clients (2)



1. IDS on gateway R detects intrusion, raises alarm to Reroute Coordinator.
2. Coordinator informs clients with new route information:
  - a) inform clients' DNS;
  - b) inform clients' network proxy server;
  - c) inform clients directly;
  - d) inform the proxy servers and ask the proxy server do (a – c).

# SCOLD: set up new indirect route (3)



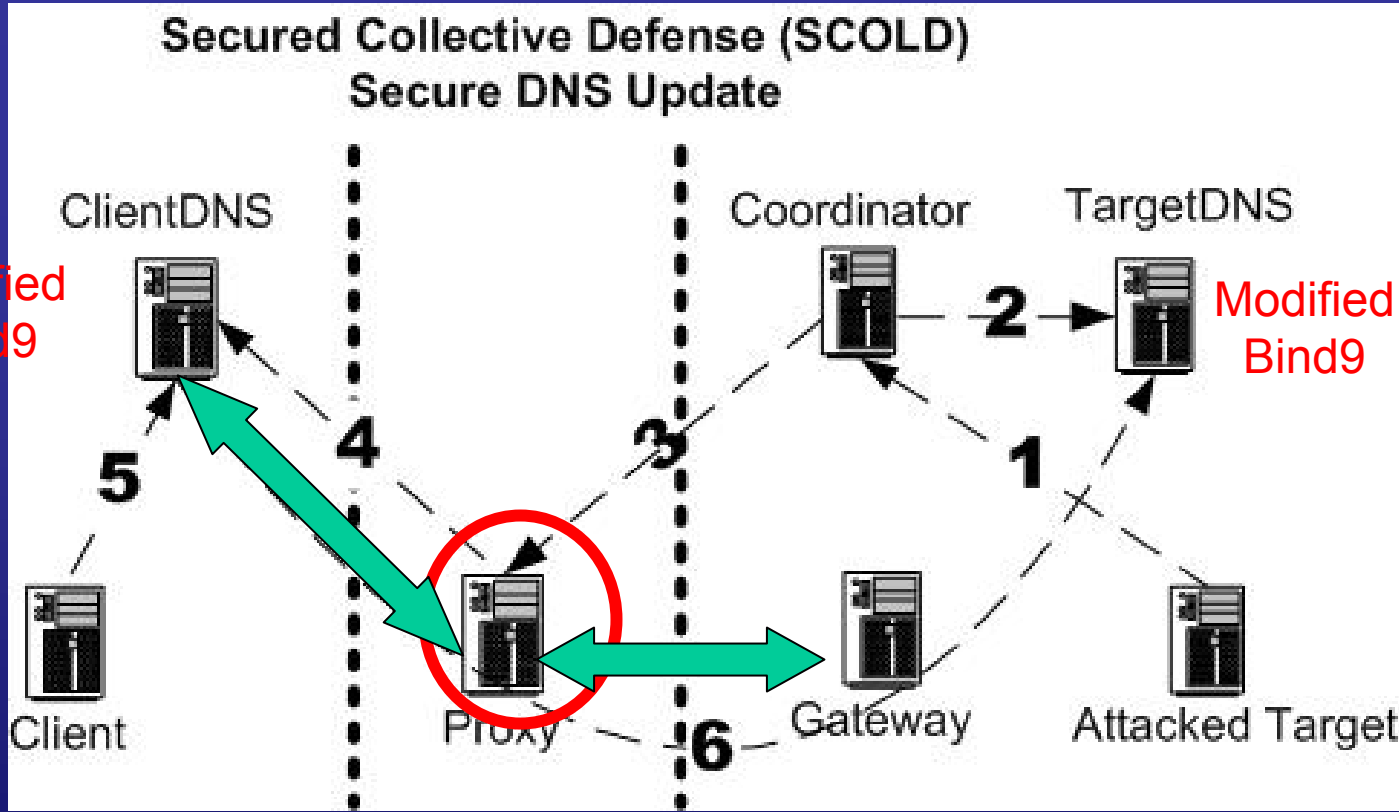
3. Clients set up new indirect route to target via proxy servers. What are proxy servers used for? a) provide alternate route and potential multiple routes; b) hide alternate gateway and reroute coordinator; c) equipped with IDS to block attacks.

# SCOLD Secure DNS Update with New Indirect DNS Entries

Major Work New Protocol

Modified Bind9

Modified Client Resolve Library



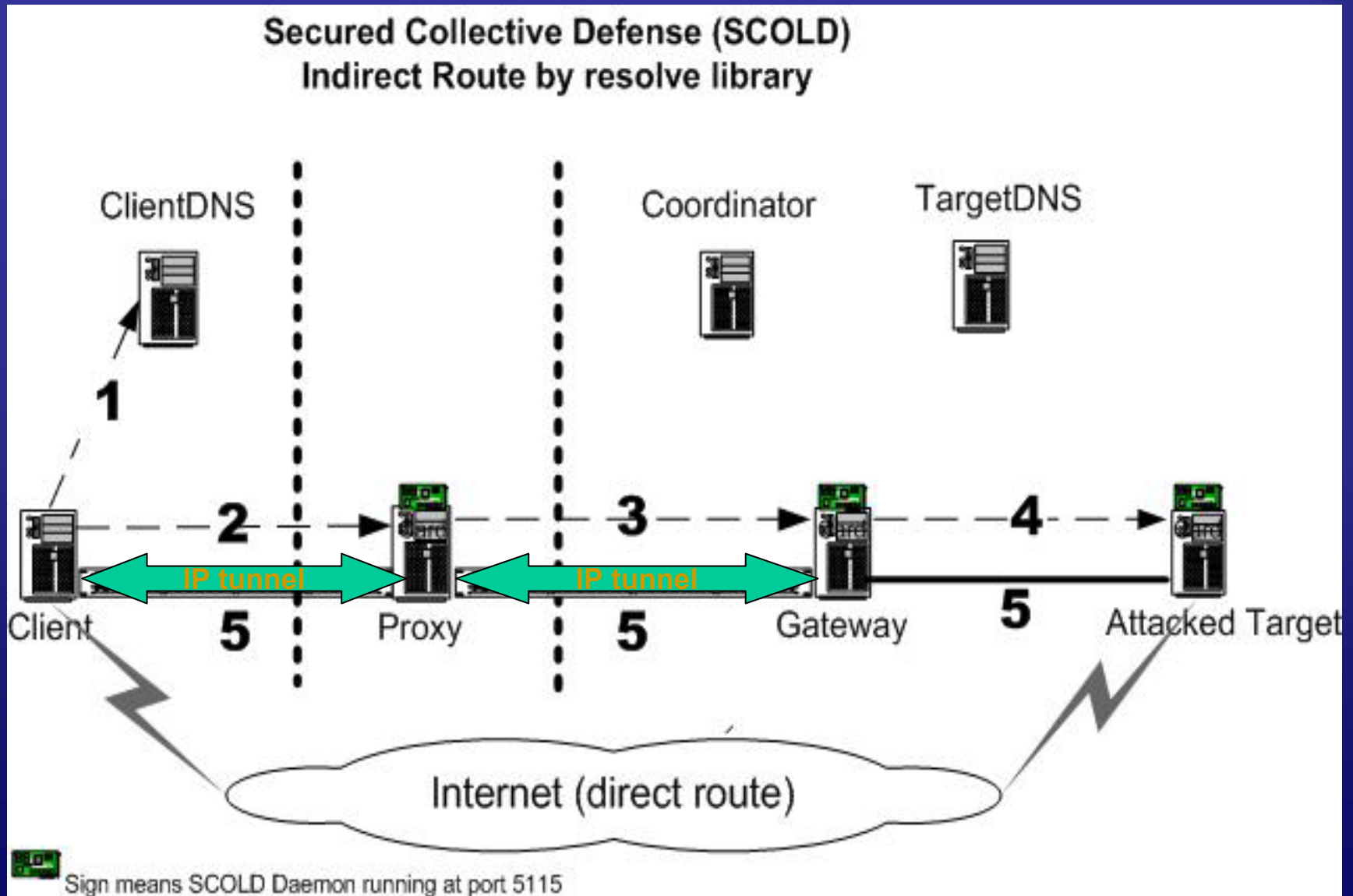
## New Indirect DNS Entries:

(target.targetnet.com,  
133.41.96.71, ALT 203.55.57.102  
203.55.57.103  
185.11.16.49  
221.46.56.38

A set of alternate proxy servers for indirect routes

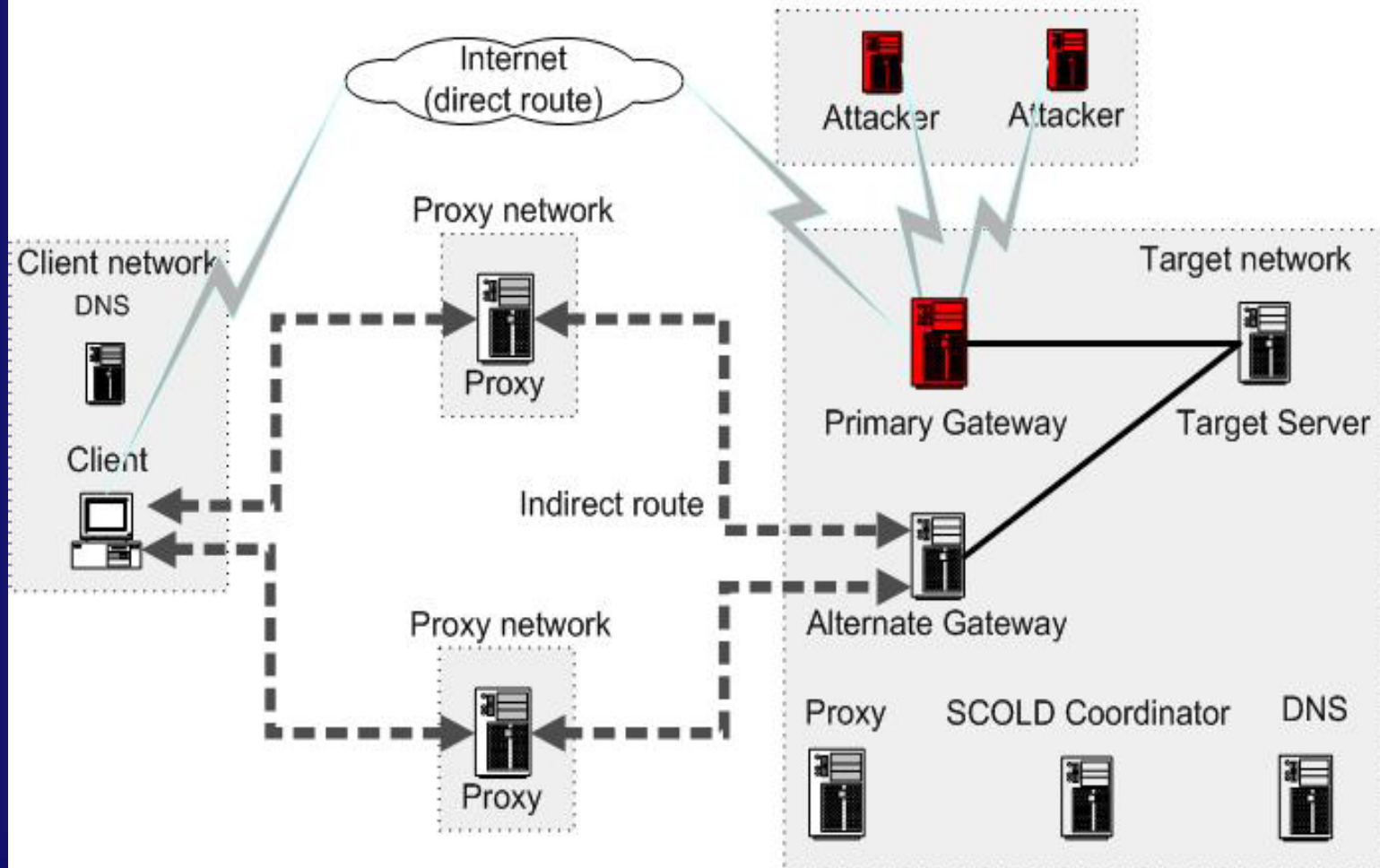
Set up indirect route for DNS update since victim DNS is subject to DDoS attacks too.

# SCOLD Indirect Routing



# SCOLD Testbed

## Secured Collective Defense (SCOLD) Testbed



# Performance of SCOLD v0.1

- Table 1: Ping Response Time (on 3 hop route)

No DDoS attack direct route	DDoS attack direct route	No DDoS attack indirect route	DDoS attack indirect route
0.49 ms	225 ms	0.65 ms	0.65 ms

- Table 2: SCOLD FTP/HTTP download Test (from client to target)

Doc	No DDoS attack,		DDoS attack,		No DDoS attack,		with DDoS attack	
	FTP	HTTP	FTP	HTTP	FTP	HTTP	FTP	HTTP
100k	0.11 s	3.8 s	8.6 s	9.1 s	0.14 s	4.6 s	0.14 s	4.6 s
250k	0.28 s	11.3 s	19.5 s	13.3 s	0.31 s	11.6 s	0.31 s	11.6 s
500k	0.65 s	30.8 s	39 s	59 s	0.66 s	31.1 s	0.67 s	31.1 s
1000k	1.16 s	62.5 s	86 s	106 s	1.15 s	59 s	1.15 s	59 s
2000k	2.34 s	121 s	167 s	232 s	2.34 s	122 s	2.34 s	123 s

# Conclusion and Future Direction

- Secure Collective Defense Network needs significant helps from community. Tremendous research and development opportunities.
- SCOLD v.01 demonstrated DDoS defense via
  - Secure DNS updates with new indirect routing
  - IP-tunnel based indirect routing to let legitimate clients come in through a set of proxy servers and alternate gateways.
  - Multiple indirect paths provide additional Internet bandwidth dynamically, not available from current Internet direct routing.
- Future works:
  - Push back intrusion traffic by using IDIP.
  - Implement multiple path connections
  - Social study on how to organize secure collective defense.