Connecting Chameleon Tenant Networks to an ExoPlex Network Service Provider

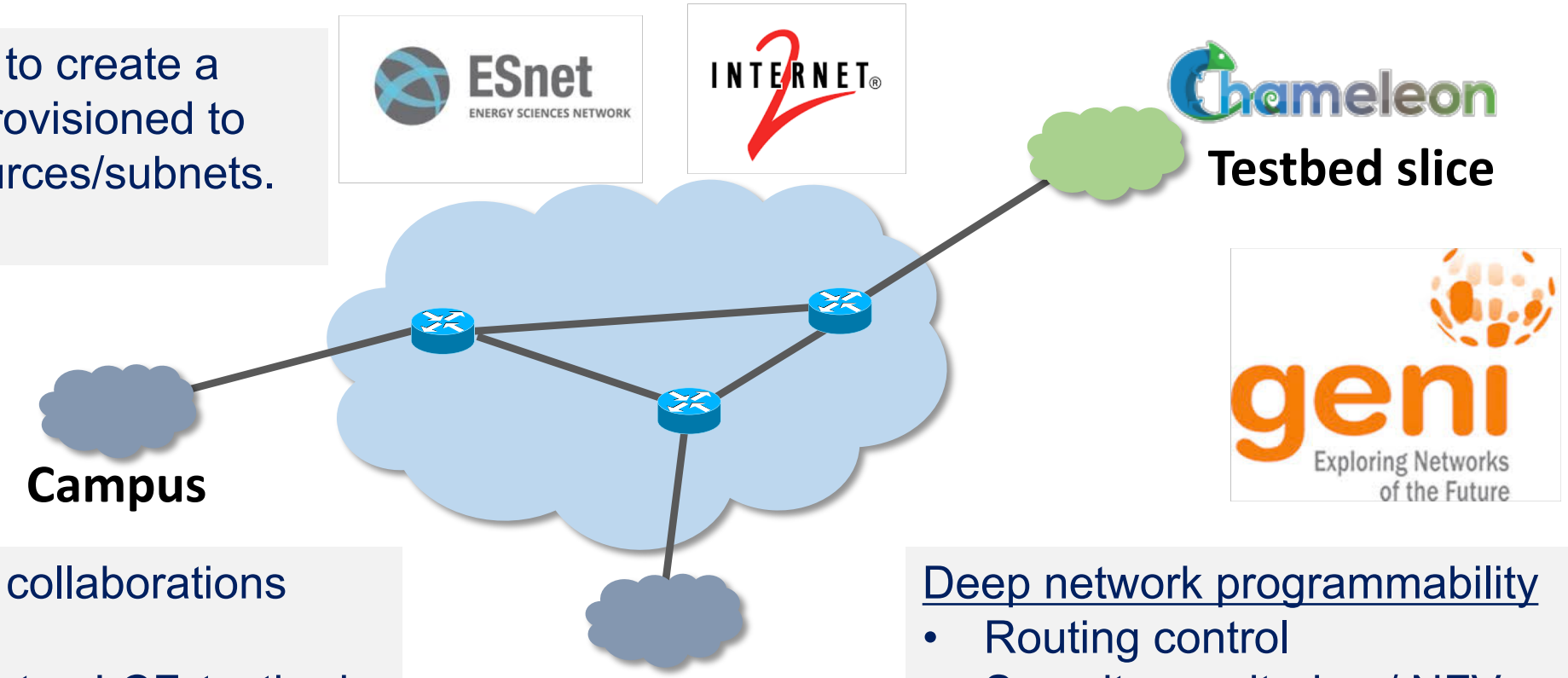
Yuanjun Yao, Qiang Cao, Rubens Farias,
Jeff Chase, Victor Orlikowski
Duke University

Paul Ruth, Mert Cevik, Cong Wang
RENCI - UNC Chapel Hill

Nick Buraglio
ESnet

Virtual Science Networks: the vision

Idea: Use circuits to create a private network provisioned to link multiple resources/subnets.
Super-facility

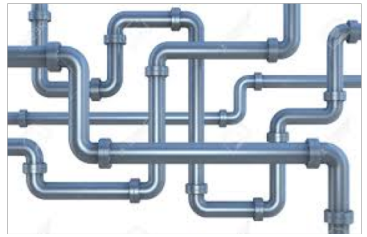


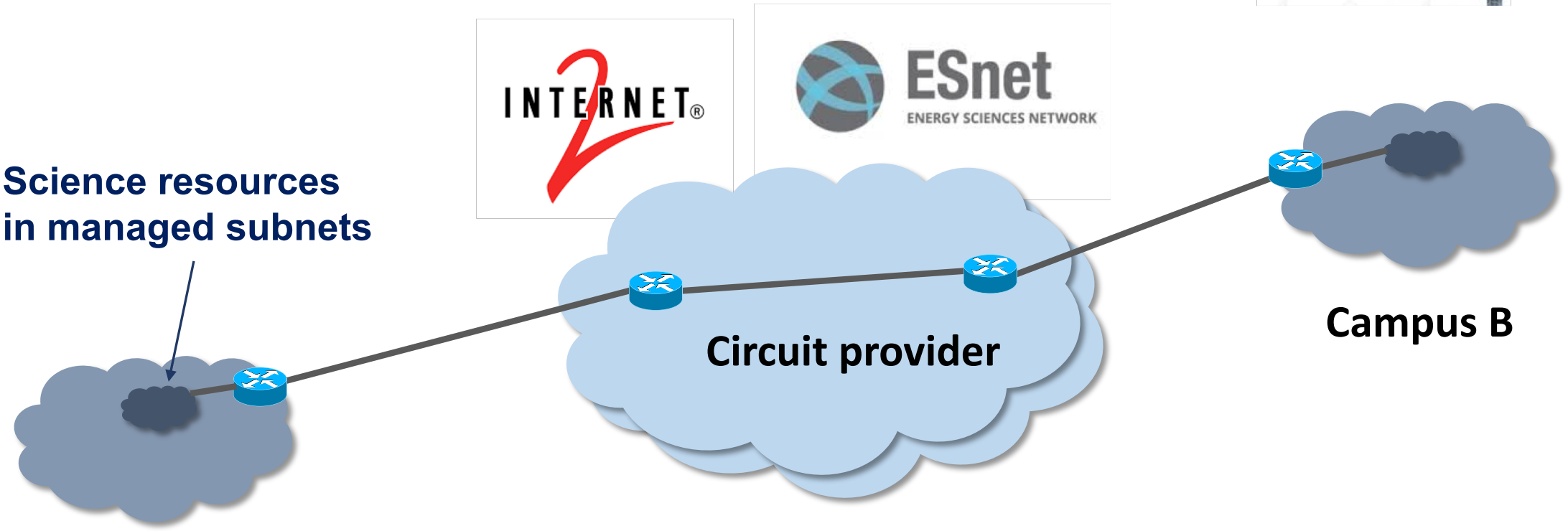
- Cross-campus collaborations
- Facility access
- **Examples**: cluster, LCF, testbed
- Resource sharing
- Virtual data enclaves
- Live network services

Deep network programmability

- Routing control
- Security monitoring / NFV
- Dynamic peering
- Topology adaptation
- Elastic edge clouds

Foundation: network circuit fabrics

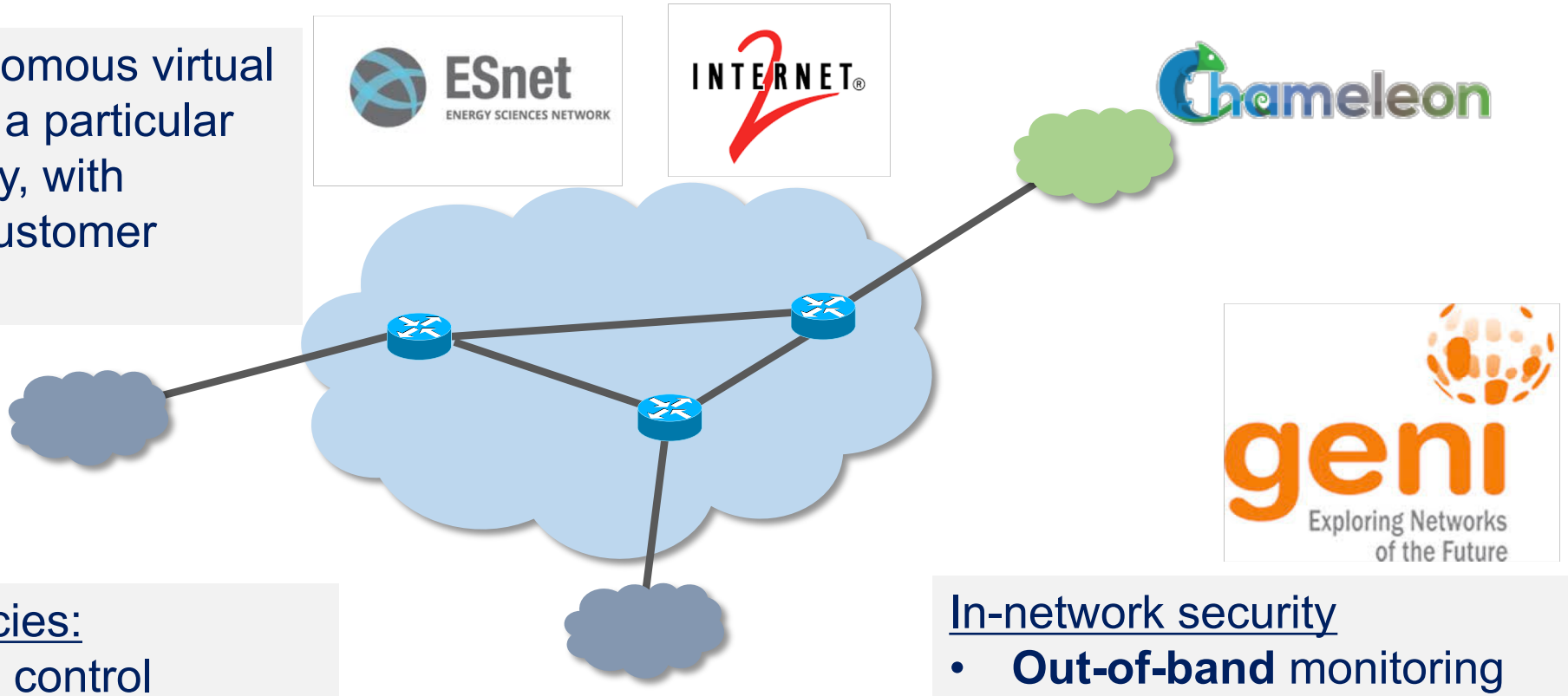




- Bandwidth-provisioned raw L2 pipes
- Dynamic on demand: edge to edge
- Programmatic hands-free IaaS APIs
  OSCARS→OESS→NSI

Security-managed virtual networks

This is a live, autonomous virtual network service for a particular research community, with multiple attached customer domains.



Edge security policies:

- Peering access control
- IP prefix ownership (“RPKI”)
- Routing authority (“BGPSEC”)
- Customer connectivity policies

In-network security

- **Out-of-band** monitoring
- **Example**: Bro IPS
- Threat-aware scanning
- Responsive traffic control

Overview: vision and approach

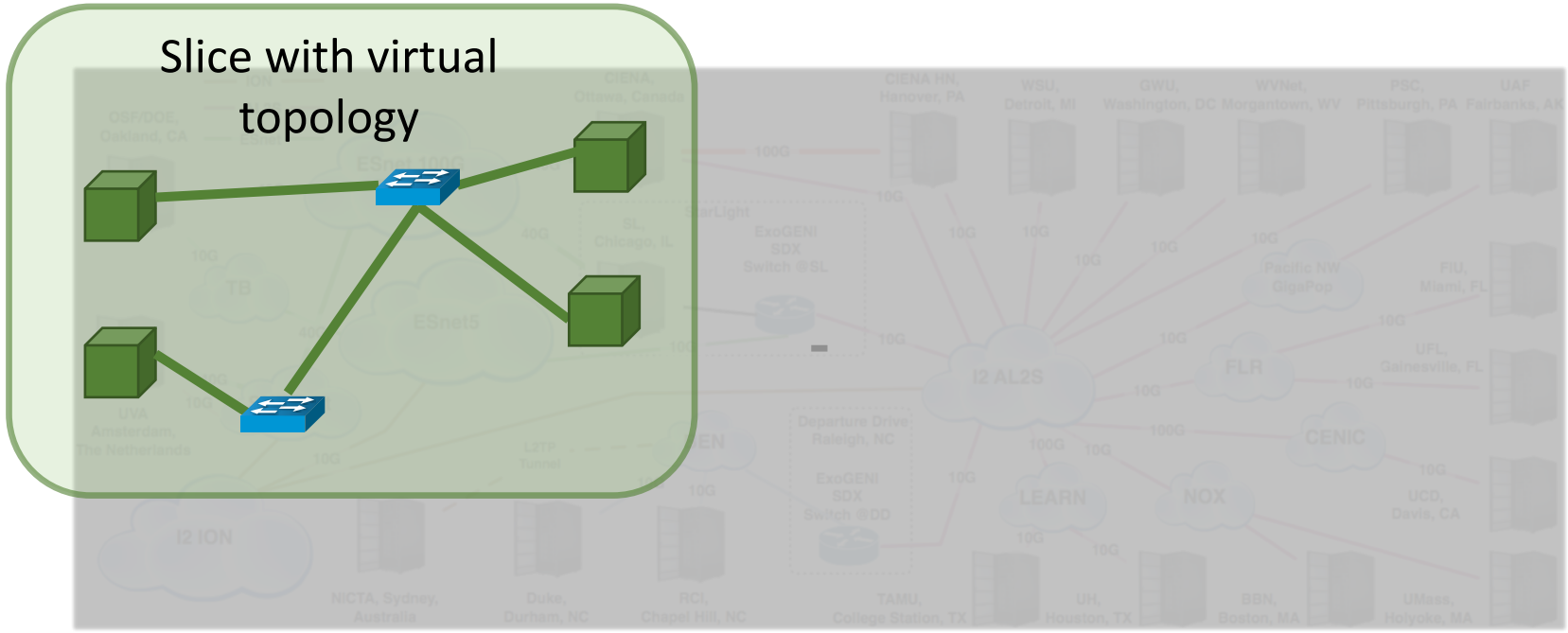
Build an architecture and platform for:

- Built-to-order **virtual science networks**
- An application of virtual Network Service Providers (vNSPs)
- Subnet-to-subnet fast-path connectivity across campus boundaries
- Security management with declarative policy, e.g., for virtual data enclaves

Elements of approach:

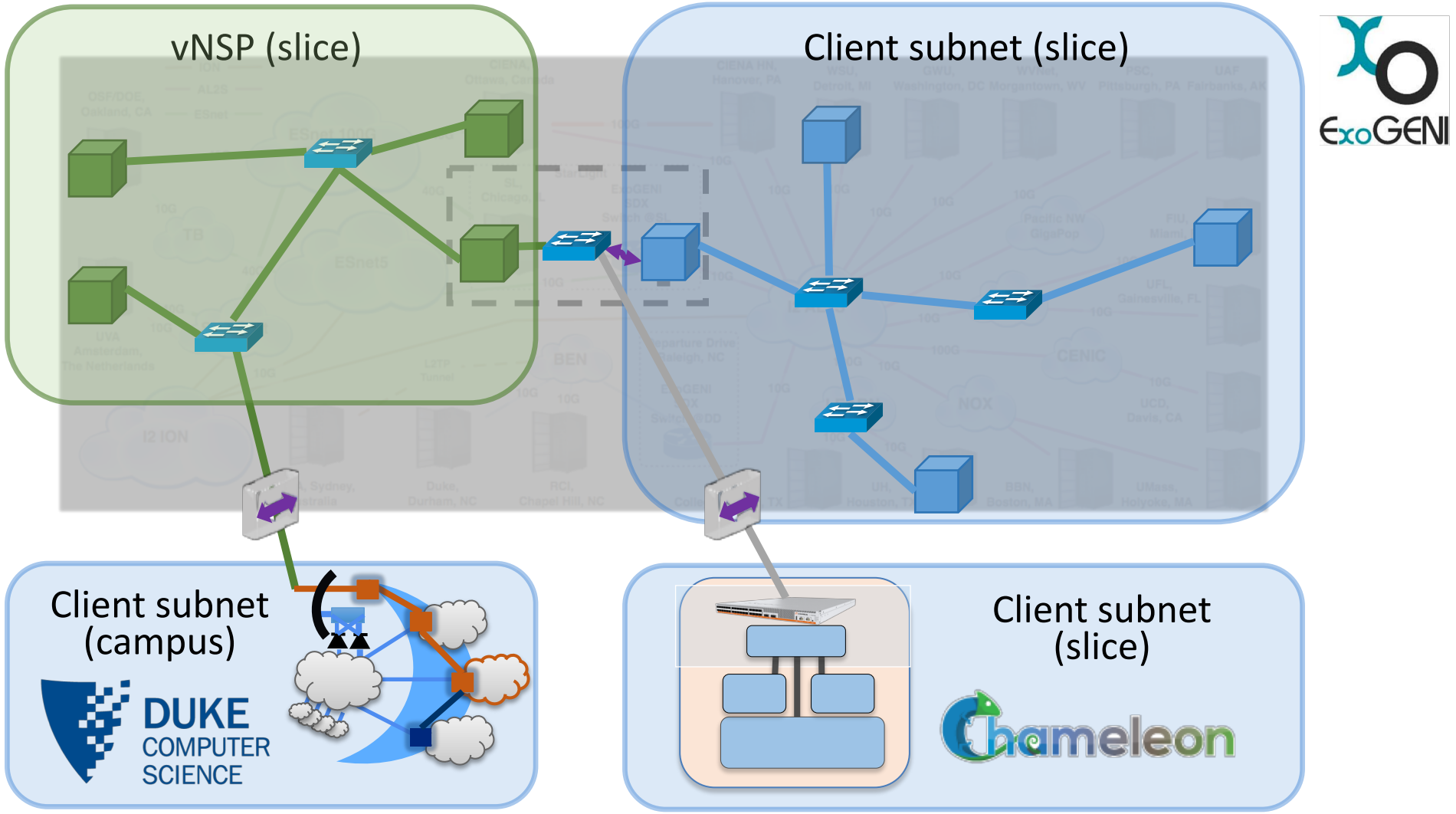
- SAFE logical trust system: logic certificates and policy rules
- Leverage national research fabrics and NSF-funded CI.
- Use GENI resources (for now) for vNSP routing and security.
- Specifically: built-to-order virtual network slices on ExoGENI

Elastic slice controllers: Ahab

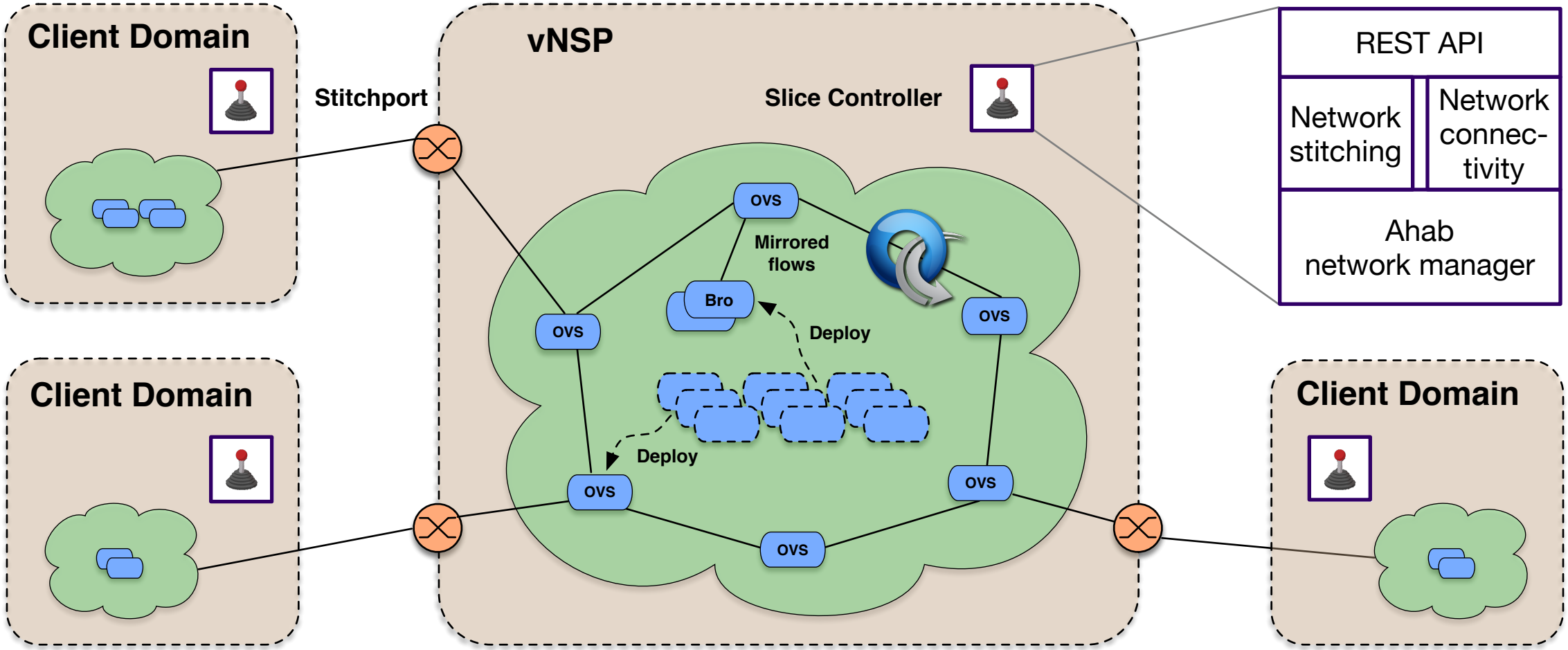


- Ahab controller architecture
- Provision VMs and pipes
- Instantiate slice and adapt the slice over time

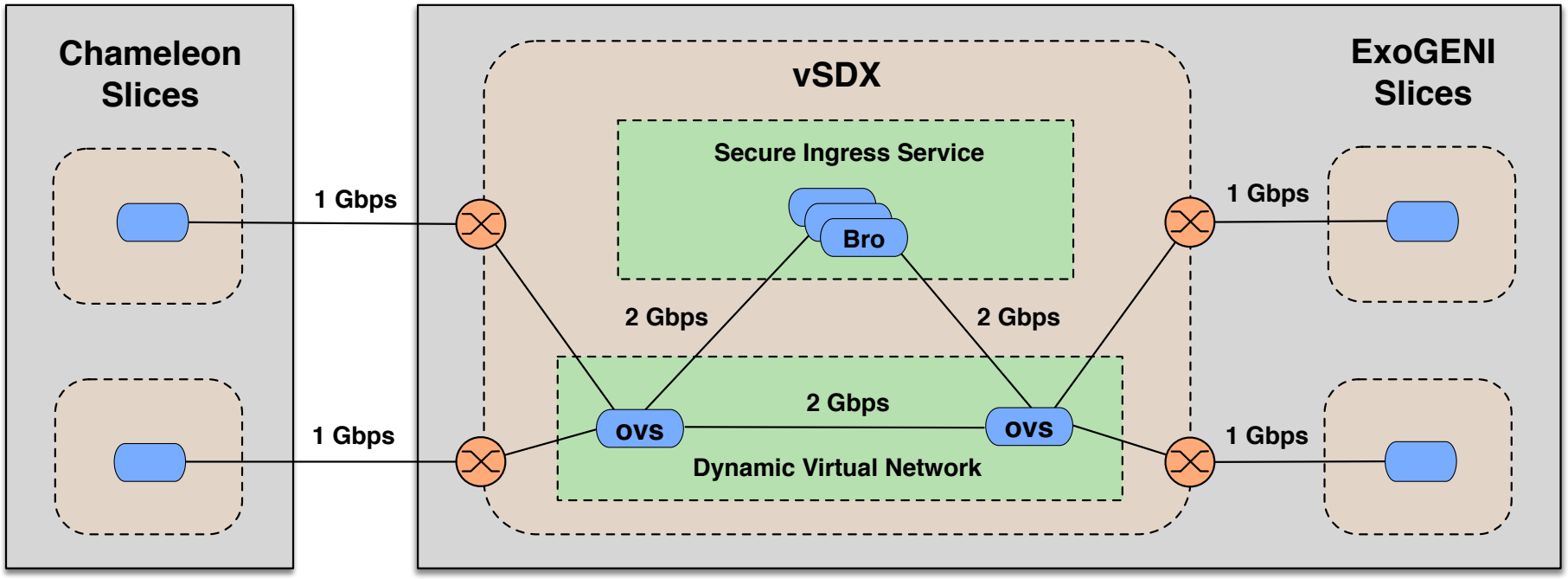
Stitching to Chameleon



ExoPlex platform

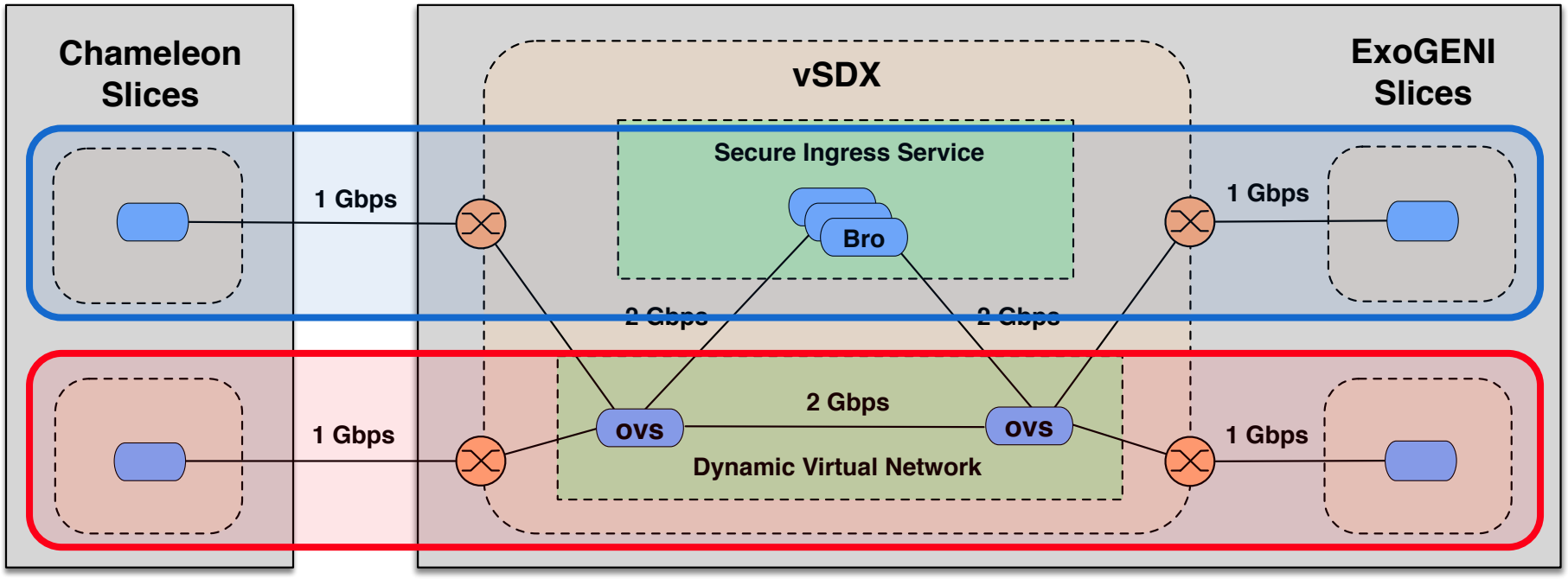


Chameleon experiment: vSDX



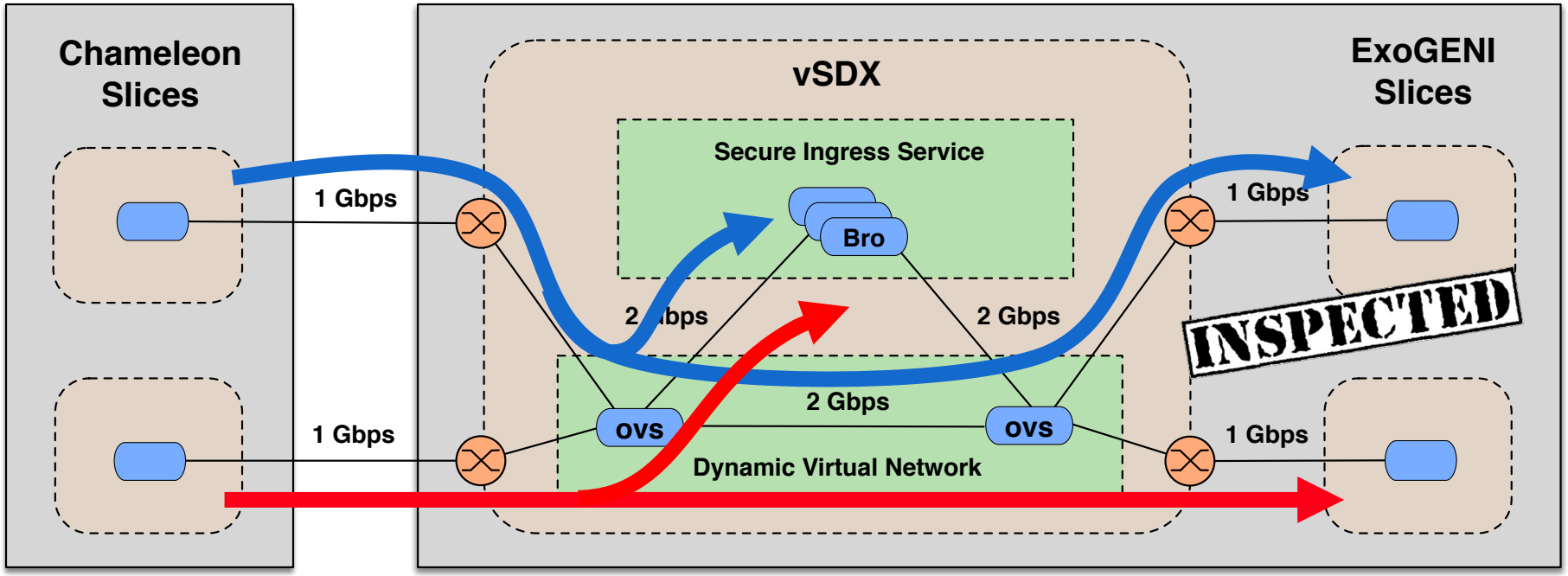
- Virtual SDX
  - **Distributed**: many points of presence to attach customers
  - **Elastic backplane**: allocate/release network resources dynamically

Example vNSP: vSDX



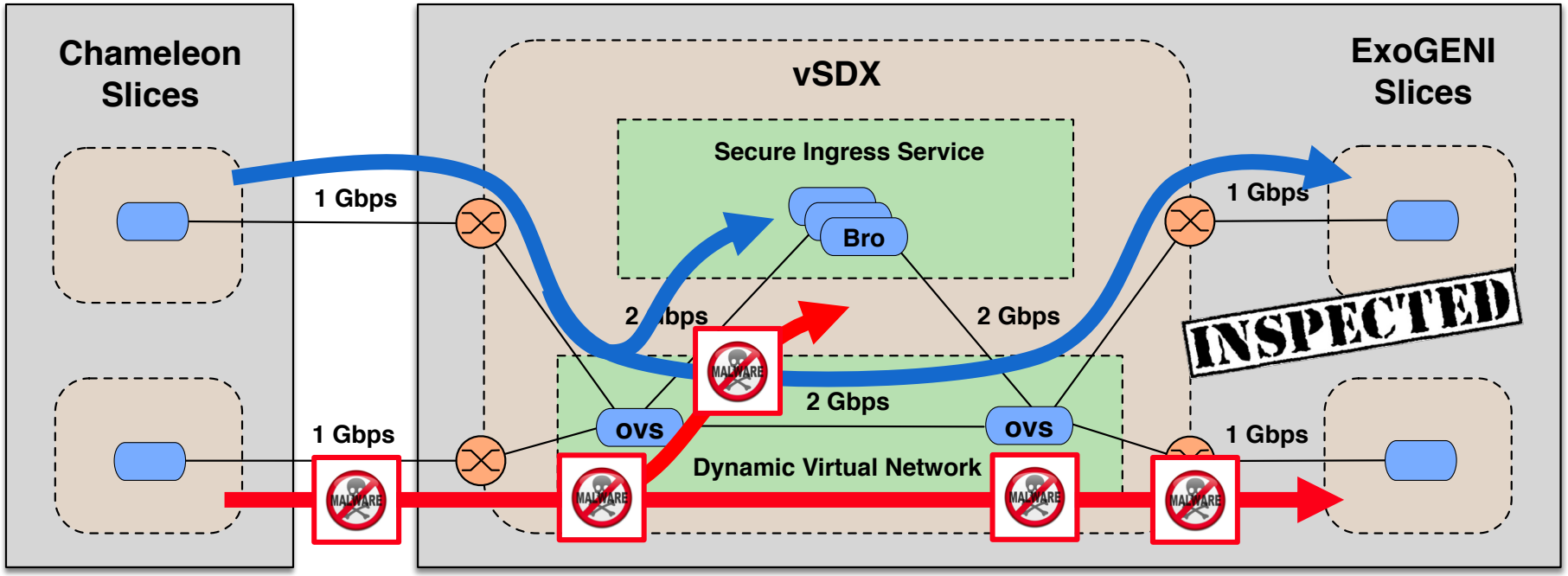
- Clients: 2 Chameleon slices, 2 ExoGENI Slices

Example vNSP: vSDX



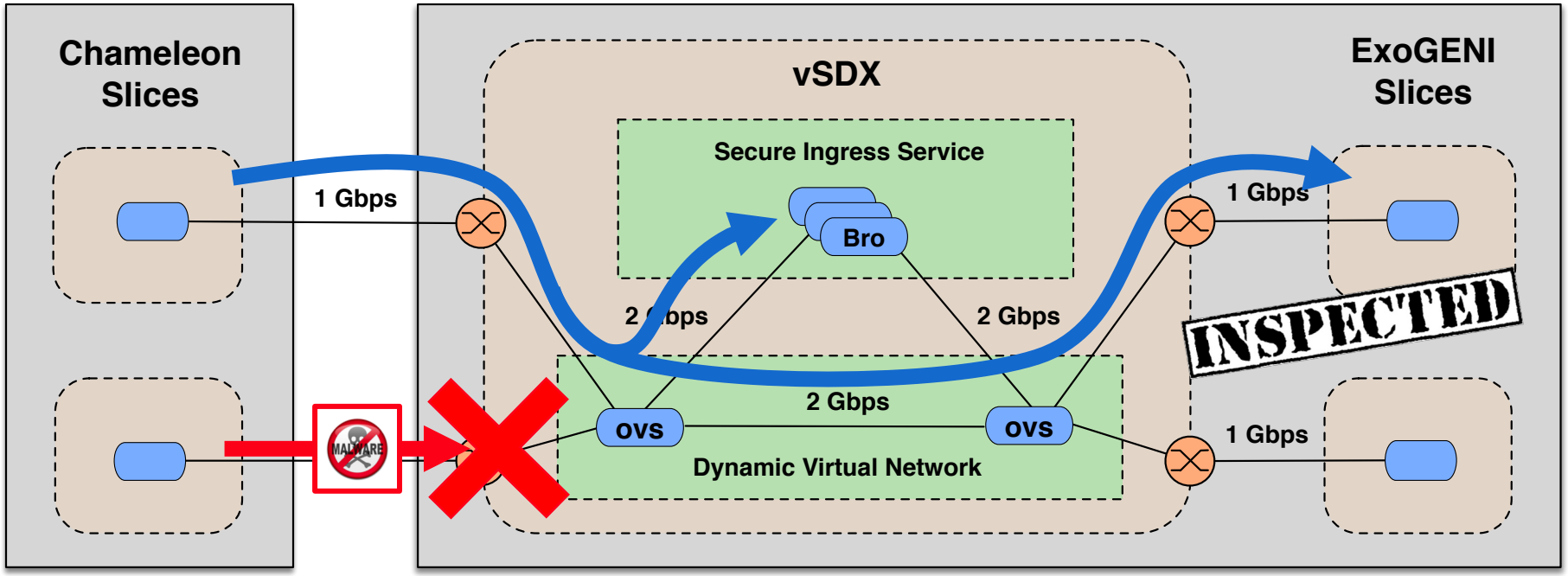
- Large file transfer

Example vNSP: vSDX



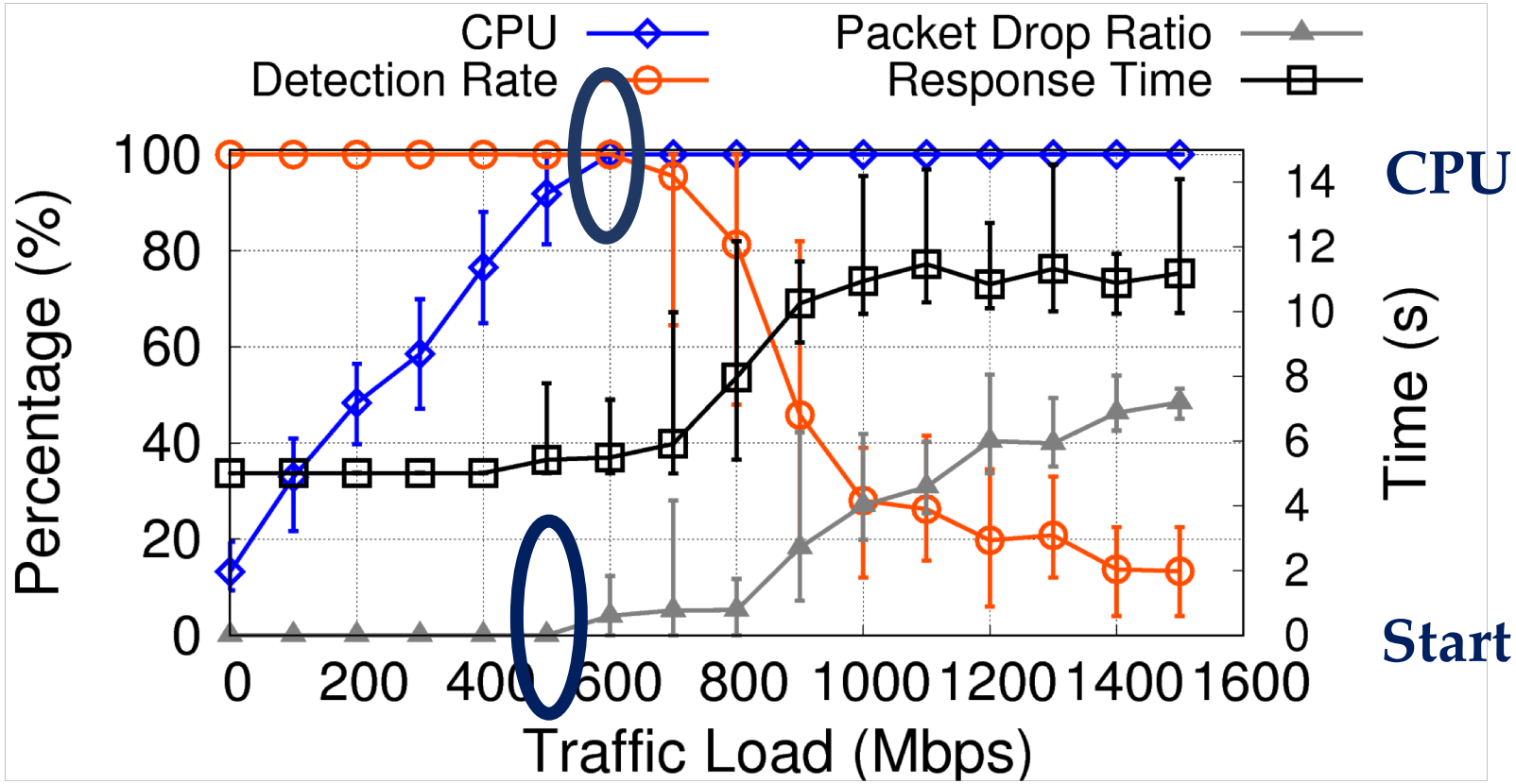
- Attack: red flow sends a malicious file with a known signature

Example vNSP: vSDX



- Bro detects malicious files
- vSDX actuates disconnection of the red flow

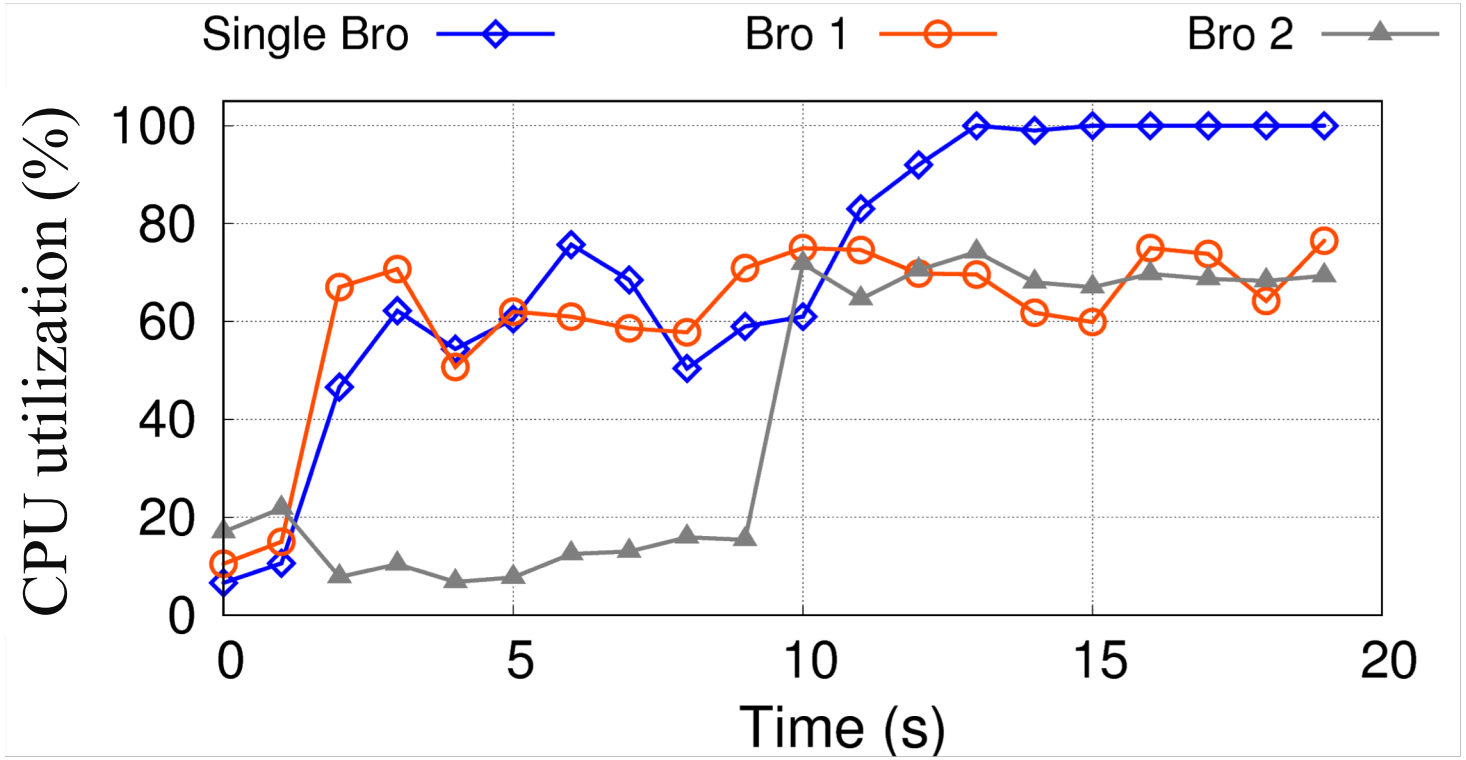
Results: Performance under load



CPU saturated

Start dropping pkts

Results: Elastic Bro deployment



- Scaling policies based on capacity and utilization

This work is partially supported by NSF awards OAC-1642140 and OAC-1642142.