Security functions capabilities exposure(Secure Routing)

Meiling Chen
China Mobile
3/27/2023

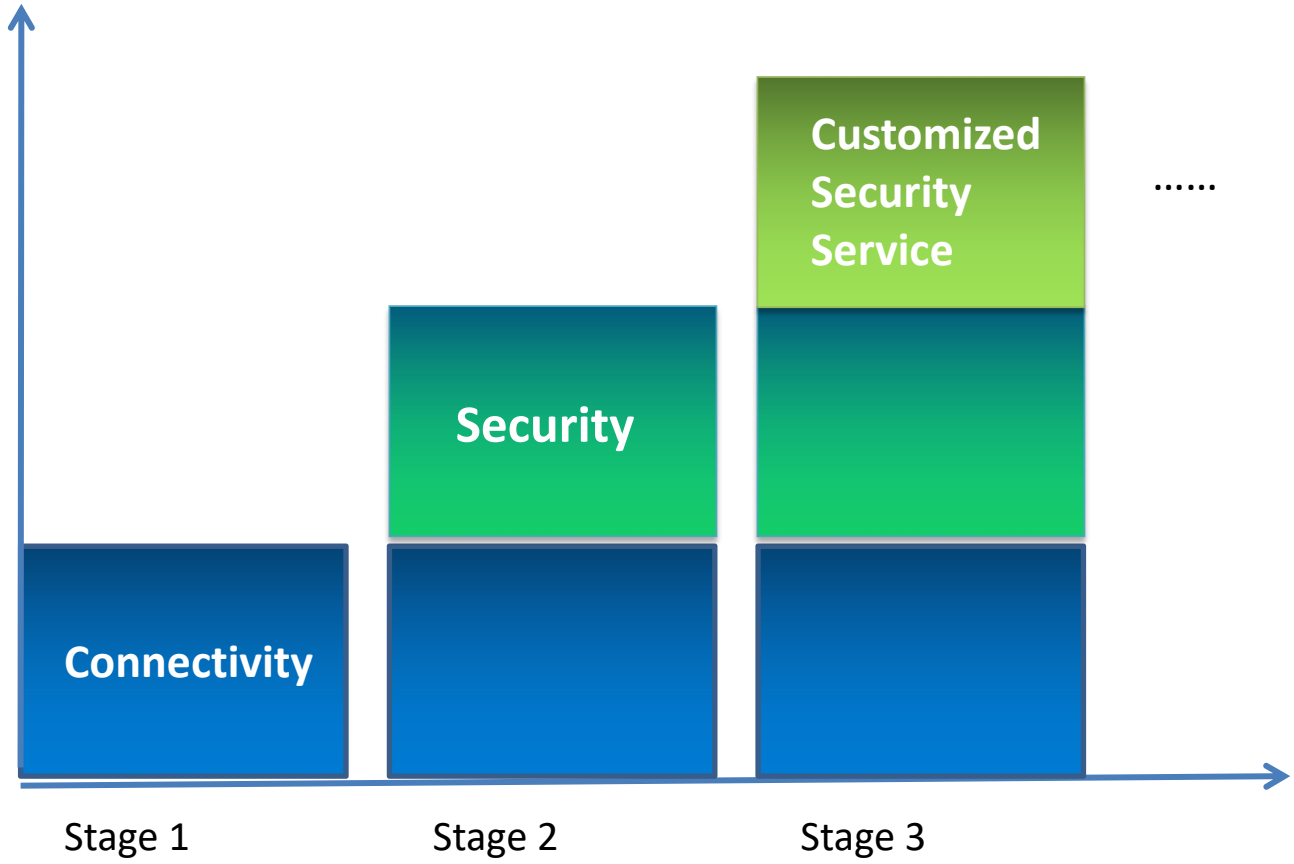
Existed Problems for security services

- China mobile has many regions (in hundreds), each regions is responsible for purchasing and deploying the security equipment independently.
  - lack the visibility across multiple regions.
  - Difficult to coordinate globally.
- To satisfiy security requirement for end-to-end services, it is necessary to know the capabilities of all security devices in all the regions.
  - Offline coodination is difficult as each region deployment status is dynamic.
- It is important to have interoperatble solution because:
  - we purchase equipment from many vendors.
  - with standard, we can easily enforce vendors to provide the exposure function during our evaluation process.

Our goal

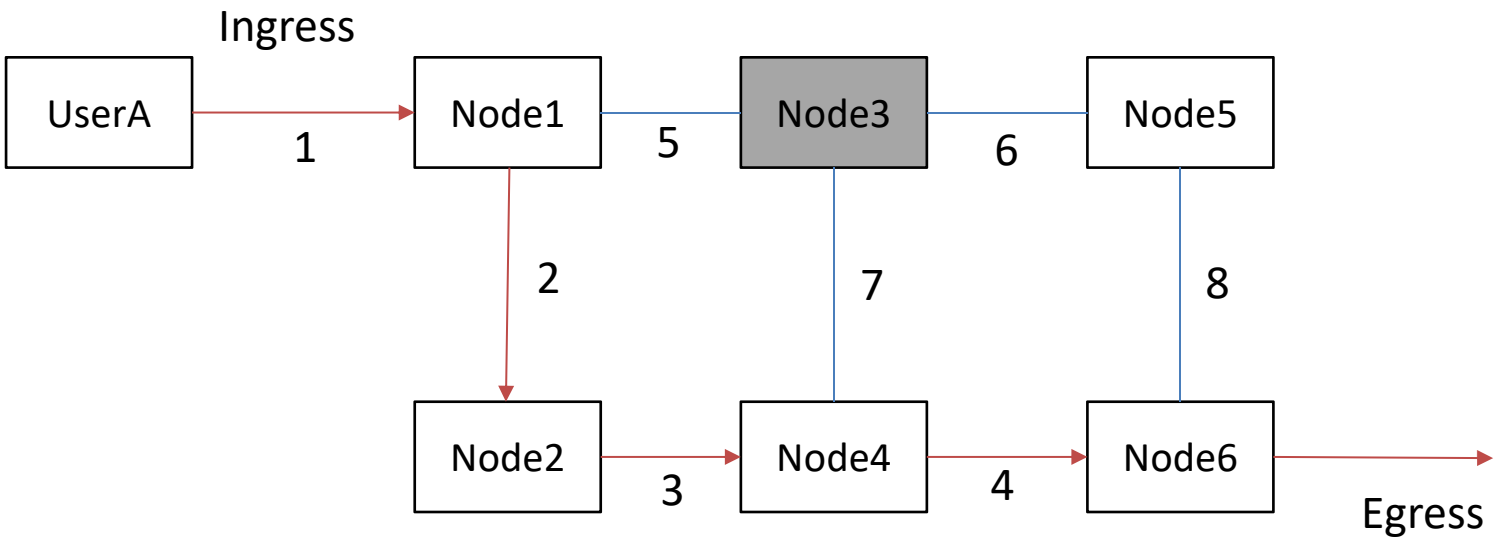
- Get community feedback
- If you are interested, please come to G304 today at 6:30pm for detailed discussion.

Evolution of user requirements for ISP



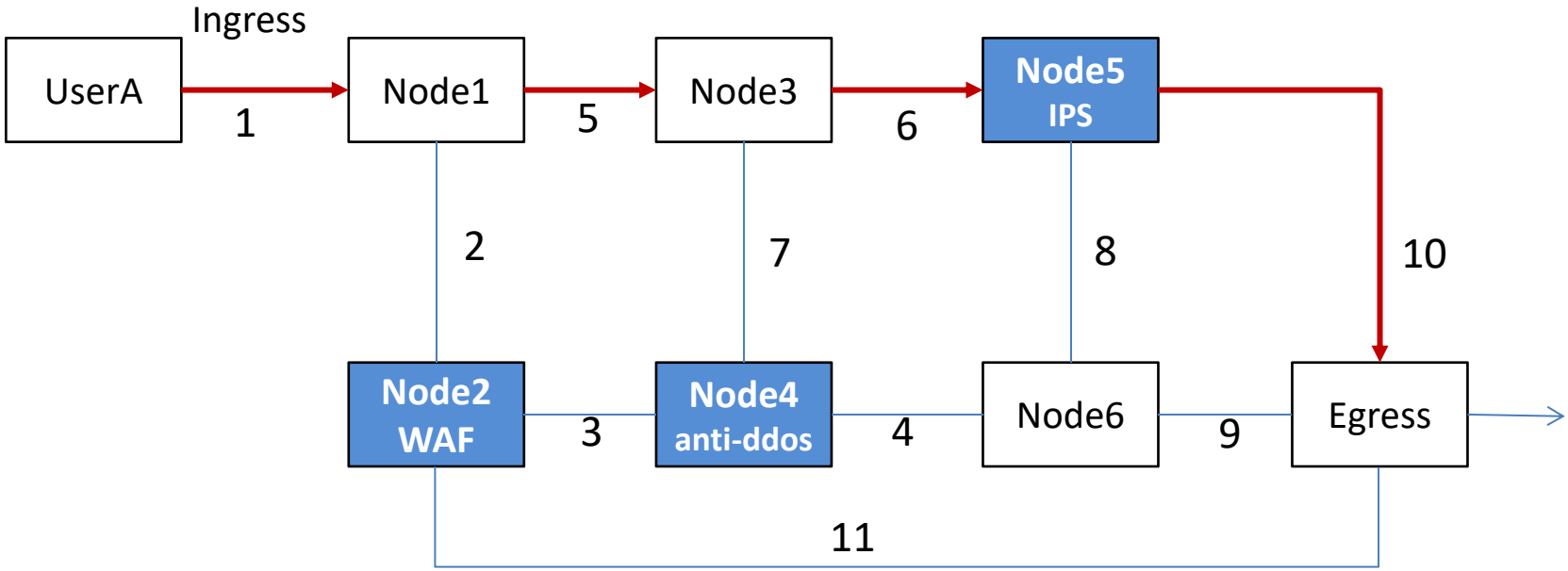
Use case1: path security (stage2)

- Based on the **security state of nodes and security functions supported by the nodes**, to form the routing path to meet the users' requirments for higher security.
  - If Node3 doesn't support specific security functions ,such as IPsec or physical isolation, or its security state isn't appraised OK, then it won't be included in the routing path for UserA.



Use case2: Customized security service(stage3)

- Based on **users' customized security requirements**, to form routing paths with corresponding various security services.
  - When userA needs IPS (Intrusion Prevention System) services, the path must pass through Node5 which provides IPS services.



Secure Routing

- **Combination of security and network:**
  - From the perspective of Carriers/ISPs, to integrate security service into the network service provided to the users.
  - From the perspective of users, the security service may include security functions like firewalls, IPS, anti-ddos, etc.

- To implement secure routing at the protocol level, some extensions of the existing protocols are needed, including:
  - Collect security information from nodes;
  - Distribute security policy via protocols, such as SRv6.

4 related drafts

1. **draft-chen-secure-routing-use-cases-02**

   https://datatracker.ietf.org/doc/html/draft-chen-secure-routing-use-cases-02

2. **draft-chen-secure-routing-requirements-01**

   https://datatracker.ietf.org/doc/html/draft-chen-secure-routing-requirements-01

3. **draft-chen-atomized-security-functions-00**

   https://datatracker.ietf.org/doc/html/draft-chen-atomized-security-functions-00

4. **draft-chen-bgp-ls-security-capability-00**

   https://datatracker.ietf.org/doc/html/draft-chen-idr-bgp-ls-security-capability-00

Next To Do

- Apply for a mailing list to dicuss the secure routing solution,
- Extend existing protocols for distributing security policy.

Comments, feedback, reviews, co-authors...