Diameter NAPT Control Application – Status Update

(draft-ietf-dime-nat-control-15)

Authors

Frank Brockners (fbrockne@cisco.com), Shwetha Bhandari (shwethab@cisco.com),

Vaneeta Singh (vaneeta.singh@gmail.com), Victor Fajardo (vf0213@gmail.com)

Key DISCUSS items from IESG

1. Behavior (and potential conflict resolution) in case a single NAT-device is controlled by multiple Controllers (possibly using different protocols).
2. Behavior in case of unexpected/unplanned termination of Diameter session.

#1 – Single NAT-device, multiple controllers

- Issue
  - In case multiple controllers (potentially using even different protocols, i.e. DNCA in parallel with SNMP and Operator-CLI) control a single device, conflicting NAT-bindings could be configured for a single endpoint.
- Approach in -15
  - Conflicts cannot occur, because the draft ***requires*** that only a single controller is responsible for a single endpoint:

> "DNCA can be deployed in different ways. DNCA supports deployments with "n" NAT-controllers and "m" NAT-devices, with n and m equal to or greater than 1. For DNCA, the session representing a particular endpoint is atomic. Any deployment MUST ensure that for every given endpoint only a single NAT-controller and only a single NAT-device are active at any point in time. This is to ensure that NAT-devices controlled by multiple NAT-controllers do not receive conflicting control requests for a particular endpoint, or would be unclear which NAT-controller to send accounting information to."

#1 – Single NAT-device, multiple controllers

- Discussion
  - How realistic is the approach in -15? Example: Operator runs DNCA, but e.g. for testing purposes wants to use CLI to configure additional bindings?
- Possible approaches
  - Leave solution as is.
  - Allow multiple controllers to control bindings and parameters for a single endpoint. Add operational considerations to the draft for this case:
    - Only allow a multiple controller scenario for the case where multiple controllers use *different* control mechanisms/protocols. I.e. we'll not cover the case where multiple DNCA NAT-Controllers control a single endpoint
    - The NAT-device needs to allow the operator to configure a policy which defines which control mechanism takes precedence in case of conflicts.

#1 – Single NAT-device, multiple controllers

DNCA can be deployed in different ways. DNCA supports deployments with "n" NAT-controllers and "m" NAT-devices, with n and m equal to or greater than 1. **From a DNCA perspective an operator MUST ensure that the session representing a particular endpoint is atomic. Any deployment MUST ensure that for any given endpoint only a single DNCA NAT-controller and is active at any point in time.** This is to ensure that NAT-devices controlled by multiple DNCA NAT-controllers do not receive conflicting control requests for a particular endpoint, or would be unclear which NAT-controller to send accounting information to.

#1 – Single NAT-device, multiple controllers

Deployment Scenarios:

Operational considerations MAY require an operator to use alternate control mechanisms or protocols such as SNMP or manual configuration via a Command-Line-Interface to apply per-endpoint NAT-specific configuration, like for example static NAT-bindings. For these cases, the NAT-device MUST allow the operator to configure a policy how configuration conflicts are resolved. Such a policy could for example specify that manually configured NAT-bindings using the Command-Line-Interface always take precedence over those configured using DNCA.

#2 - Unexpected/unplanned termination of Diameter session

- Issue
  - The behavior in case the DNCA peer in the NAT-device or NAT-controller crashes isn't fully specified. Stale NAT-bindings in the NAT-device may result in case the Diameter session is lost.
- Requirement
  - Mechanism at the NAT device to detect the Diameter session being aborted and take action to "cleanup" the existing state for the session.
  - Note that the "cleanup" action can be used for DoS attacks, because loss of the Diameter session immediately leads to a loss of connectivity: Operator should be given the option to configure how quickly the state is cleaned up, i.e. cleanup can be immediate following a session abort detection or timer based.

#2 - Unexpected/unplanned termination of Diameter session

Session Establishment/Management:

Authorization-Lifetime AVP (RFC 3588 Section 8.9) in the NC-Request MUST be used to specify the validity of the NAT-bindings at the time of its creation. The validity of the NAT-bindings associated with a DNCA session MUST be extended after successful re-authorization of the session. When Diameter session is detected to be dead (e.g. due to failure in reauthorization, due to a note from Diameter watchdog etc.), NAT-bindings pertaining to that session will be cleaned up after a configured grace period or after a period as specified in Auth-Grace-Period AVP in NC-Request message. The grace period can be configured as zero or higher based on operator preference.

#2 - Unexpected/unplanned termination of Diameter session

Failure cases of the DNCA Diameter peers:

If session reauthorization fails NAT-bindings pertaining to that session MUST be cleaned up after a configured grace period or after a period as specified in Auth-Grace-Period AVP in NC-Request message. The grace period can be configured as zero or higher based on operator preference.

#2 - Unexpected/unplanned termination of Diameter session

Security section:

In addition, the operator needs to consider security threats resulting from unplanned termination of the DNCA session. Unplanned session termination, which could e.g. happen due to an attacker taking down the NAT-controller, leads to the NAT-device cleaning up the state associated with this session after a grace period. If the grace period is set to zero, the endpoint will experience an immediate loss of connectivity to services reachable through the NAT-device following the termination of the DNCA session.