Trust Networking and Procedures for Autonomic Networking

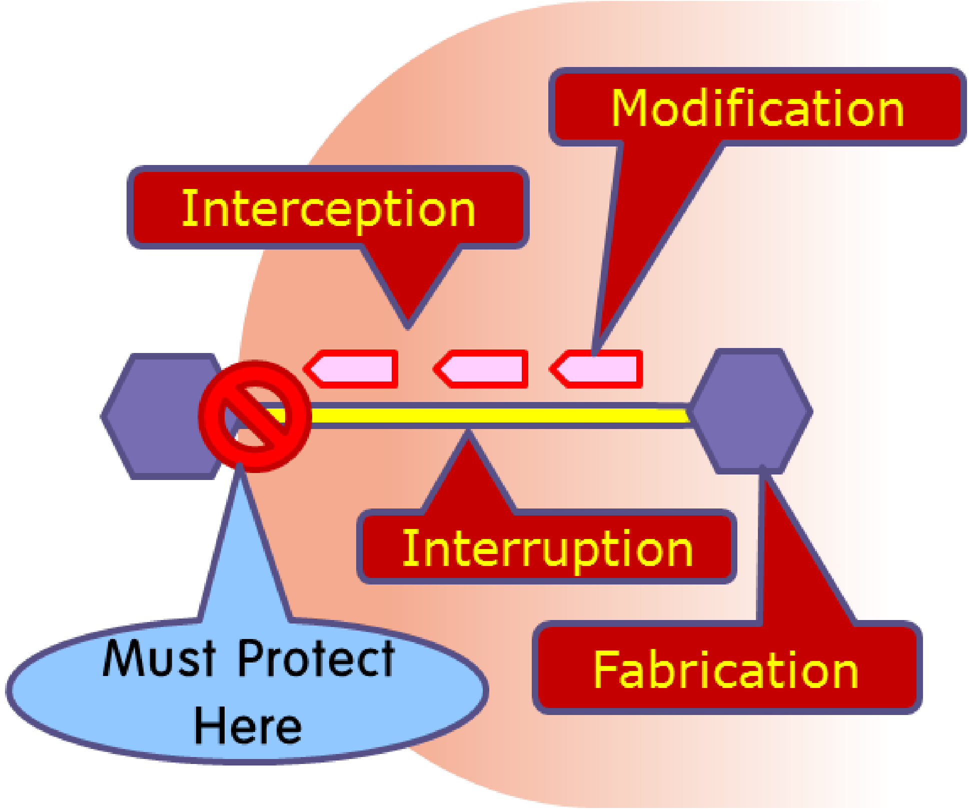
draft-choi-anima-trust-networking-00

July 18, 2018

Taesang Choi, Taesoo Chung, ETRI
Junkyun Choi, Jaeseop Han, Woojik Chun, KAIST

TN Background: Security Model & Limitations

- The security model of the current Internet is based on the assumption that all traffic coming from the Internet is suspicious.
- The lack of inherent security in IP protocol has led various attacks, such as attack on confidentiality by intercepting packets, integrity attack by modifying of the contents of packets, authentication attack by identity fabrication, and availability attack by interfering normal communicatio ns.
- In the context of untrusty Internet, each host should protect itself from potential risks of the hostile Internet. This protection usually take place at the final destination as seen in Figure
- This model operates basically in reactive manner. That means, after rec eiving all arriving packets, threatening packets can be detected and re moved
- Detection of threatening packets are based on pre-defined rules extrac ted from previous attacks. The reactive operations of security model re sult in endless malicious cycle of attacks and defenses
- Rules has to be upgraded for every newly discovered attacks and more complicate rules are required as more sophisticate attacks emerge
- This model is fatal in the case of devices with limited or no processing power. Also stronger security makes the system weaker in defending D oS (Denial of Service) attacks.



TN Background: Security Model vs Trust Model

- The trust model is based on confidence that entities in a trust networking domain never do harm, while the security model is based on suspicion that adversaries attacks anytime
- The relationship in trust model is binary in the sense that an entity trust another specific entity, but relationship in the security model is unary because the entity itself must protect regardless of other entities
- With respect of rules, trust model keeps trusted IDs as a white list but security model keeps threatening entities as a black list
- Thus, behavior of entities in the trust model is proactive while the security model acts in reactive manner
- That leads the policy of the trust model is to prevent risk by communicating only with trusted entities, but policy of the security model monitors all communications to detect and remove threatening actions
- The trust model provides mechanisms for accepting entities or domains after verifying their trust, while the security model provides mechanisms for watching the traffic and blocking the threatening traffics
- As the result, the network space of the trust model starts with a restricted space and incrementally glows as new entities or domains are accepted, while the network space of security model starts as an unrestricted and open space, but the space may be diminished by excluding misbehaving entities

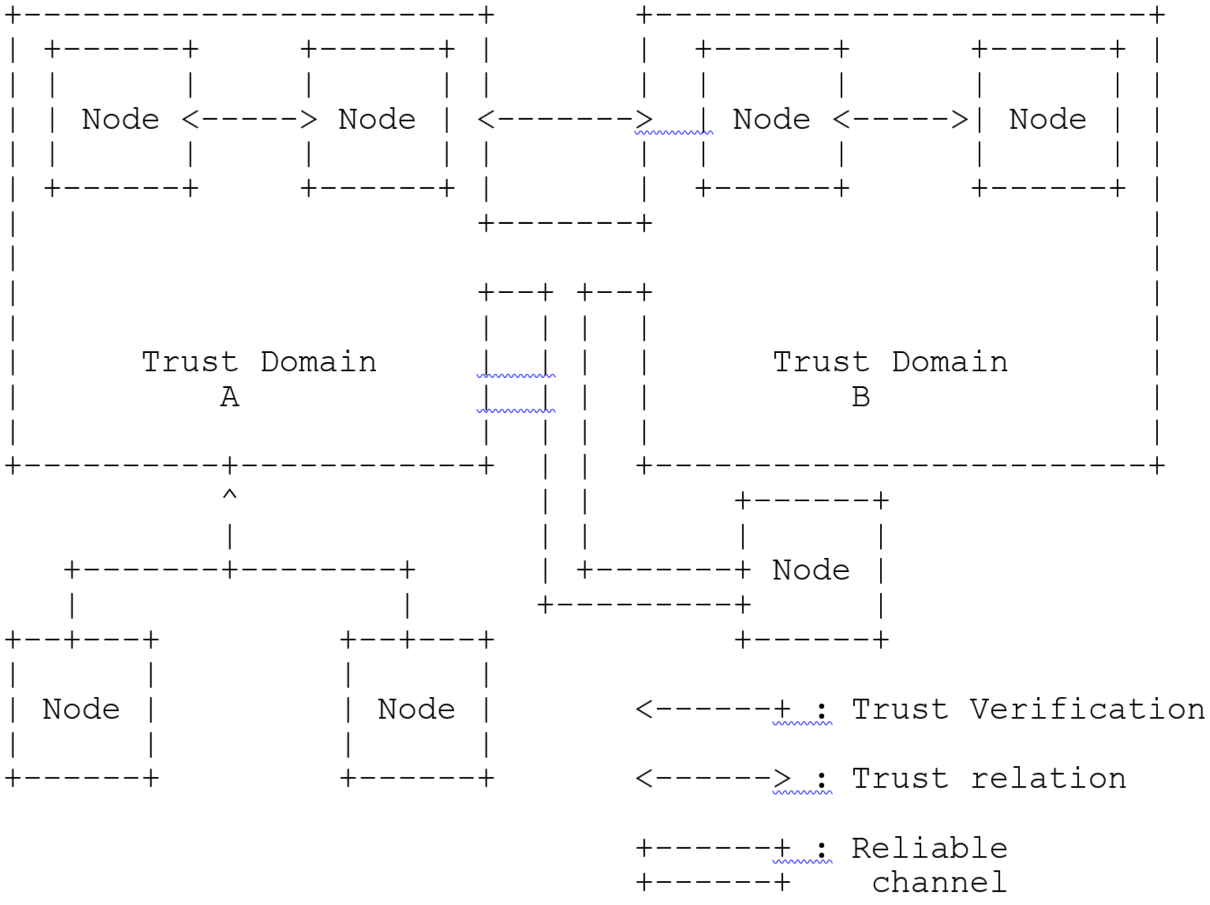
	Trust Model	Security Model
based on	confidence	suspicion
relationship	binary	unary
rules	white list	black list
behavior	proactive	reactive
policy	prevention	detect and remove
mechanism	verify and accept	watch and block
network space	unrestricted and diminishing	restricted and expanding

Trust Networking Domain (TND)

- Objective
  - To provide trustworthy communication network infrastructure
- Autonomic Domain with respect to “trust”
  - A collection of autonomic nodes, which trust each other (with the same intent, i.e. trust)
  - Hosts and Communicating elements as autonomic nodes
    - Trust-bootstrap: verify trustworthiness and register
  - Trust Manager as Registrar
  - Domain gateway
    - The autonomic node that has “inter-domain communication” Autonomic Service Agent(ASA)
- Backward Compatibility
  - Legacy host (IP device) should be supported with little modification
  - Legacy hosts communicate with only local IP addresses
    - Within a domain, the local IP address is used as an ID (as well as locator)
    - For inter-domain communication, ID for the host is used

Trust Networking Domain (TND)

- Definition of TND
  - the network space that is autonomous, isolated, and well protected from external attacks
- Protection of TND
  - each domain has at least one gateway that performs security functions for the domain. The gateway identifies external entities, evaluate trust level, accepts or rejects the packets according to the trust levels of external entities
- Expansion of TND
  - 3 ways how to expand the domain. First, new entities can join to the domain after passing trust verification. Second, a remote entity can join to the domain via reliable channel. And third, when two domains may have trust agreement and connected by reliable channel, all entities in one domain can exchange packets with another in the pre-agreed trust level
- Communication with external Domain
  - all communication with external entities must take place through a domain gateway, which enforces well-defined procedure communication for external entities



Node
Node
Node
Node
Trust Domain A
Trust Domain B
Node
Node
Node
<------+ : Trust Verification
<------> : Trust relation
+------+ : Reliable channel
+------+

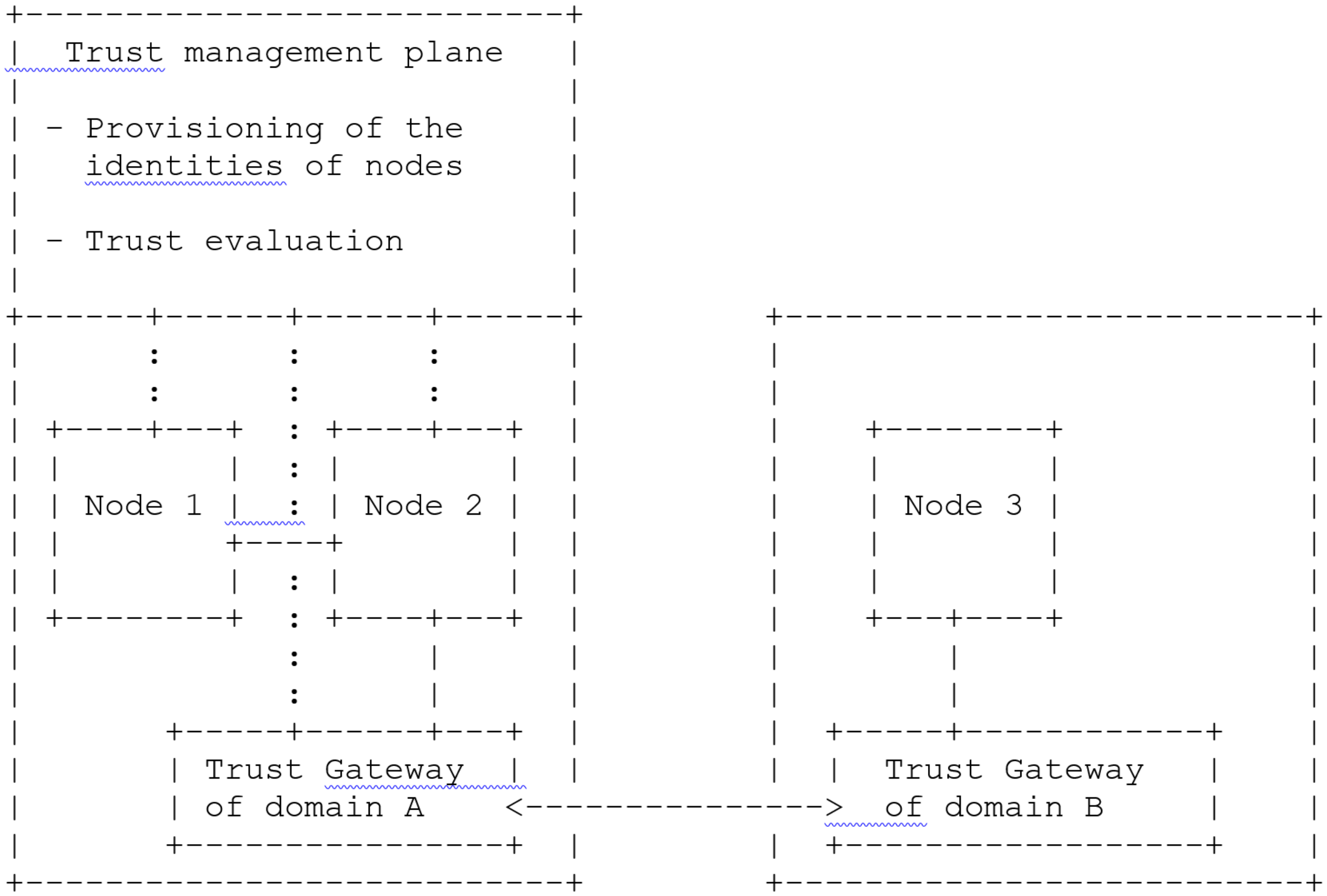
TND as an Application of ANIMA: Definition

- Node is trusted autonomic node
- Trust gateway function is a kind of ASA
- Since all nodes within a trust networking domain maintains certain trust level set by the domain, communications within the domain can be done without any further security concern
- Communications with external node require additional verification phase before the communications actually begin
- The verification is performed at the border of the domain, where external nodes are checked if their trust level are sufficiently high for the domain

```
+-----------------------------------------------+
:                                               :
:             Trust networking domain           :
:                                               :    +------------
:                                               :    :
:                                               :    :
: +---------------------------+  +-------------+:    :
: :     Autonomic Function    :  :Trust Gateway::    :
: :              :            :  :  Function   ::    :
: :     ASA 1    :     ASA 1  :  :    ASA 2    ::    :
: :              :            :  :             ::    :
: +---------------------------+  +--------------:    :
: :              :            :  :             ::    :
: +--------------------------------------------+:    :
: :                                            ::    :
: :     Autonomic Networking Infrastructure    ::    :
: +--------------------------------------------+:    :
: :              :            :  :             ::    :
: :  +---------+ : +---------+:  : +---------+ ::    : +---------+
: :  : Trusted : : : Trusted ::  : : Trusted : ::    : : External:
: :  :Autonomic:---:Autonomic:-...-:Autonomic:---------:  Node   :
: :  :  Node 1 : : : Node 2  ::  : : Node N  : ::    : :         :
: :  +---------+ : +---------+:  : +---------+ ::    : +---------+
: :              :            :  :             ::    :
+-----------------------------------------------+    +------------
```

TND as an Application of ANIMA: Configuration

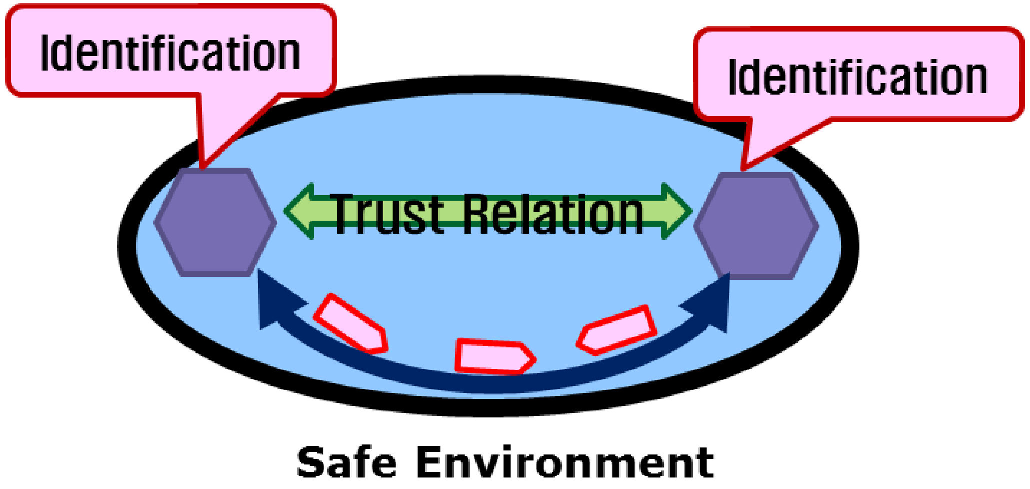
- Within a trust networking domain, an autonomic node is credited by their trust level from management plane
- The trust management plane maintains the trust information tables up to date
- The trust management plane is tracking of trust status of each autonomic node as an application of autonomic networking
- The trust information table contains the trust information of autonomic nodes based on the trust networking domain
- All the interactions between autonomic nodes should be verified according to trust evaluation procedures of management plane



```
+---------------------------+
|  Trust management plane   |
|                           |
| - Provisioning of the     |
|   identities of nodes     |
|                           |
| - Trust evaluation        |
|                           |
+------+------+------+------+         +--------------------------+
|      :      :      :      |         |                          |
|      :      :      :      |         |                          |
| +----+---+  : +----+---+  |         |    +--------+            |
| |        |  : |        |  |         |    |        |            |
| | Node 1 |  : | Node 2 |  |         |    | Node 3 |            |
| |        +----+        |  |         |    |        |            |
| |        |  : |        |  |         |    |        |            |
| +--------+  : +----+---+  |         |    +---+----+            |
|             :      |      |         |        |                 |
|             :      |      |         |        |                 |
|       +-----+------+---+  |         |  +-----+------------+    |
|       | Trust Gateway  |  |         |  |  Trust Gateway   |    |
|       | of domain A    <--------------->  of domain B     |    |
|       +----------------+  |         |  +------------------+    |
+---------------------------+         +--------------------------+
```

TND as an Application of ANIMA: Identification

- In a trust networking domain, each autonomic node should be identified by self-certifying ID (SCID), which provides secure binding between ID and key of an entity.
- Every node has a <private, public> key pair and hash of the public key is defined as the self-certified ID of the node.
- This ID can be used in validity check of claimed key against actual public key of the entity. The valid public key is basis of further identity verification.
- After identification the entity check trust relation with the peer entity so that only trusted entity is allowed to communicate.
- The trust relation used in the trust model is assumed to be reflexive, symmetric, and transitive.
- If all entities in a given group satisfy all three characteristics, the group is declared as a trust equivalent class.



TND as an Application of ANIMA: Discovery & Signalling

- The trust management information database is used for the discovery of autonomic nodes at the same trust networking domain.
- The autonomic nodes with the same trust networking domain may use the relevant identification schemes.
- In the trust management information database, a list of autonomic nodes are classified into the r elevant identification code which indicates the same trust networking domain.
- The identification code for a trust networking domain may contain name/nickname and number as well as IP address and port number, etc.
- After discovery of destination autonomic node, the signaling protocol GRASP can be used to initia te data exchange. Specifics are for further study.
- Within the same trust networking domain, an autonomic node directly communicates with each other after completing signaling procedure, in which the connectivity among autonomic nodes ar e securely and automatically maintained.
- The pre-configuration between autonomic nodes can be done during bootstrapping.
- For data exchange with different trust networking domains or non-autonomic nodes, the trust gat eway provides proper interworking functions for data exchange and signaling since there is no dir ect communication paths between them

TND as an Application of ANIMA: Evaluation

- Trust evaluation of network is the way of calculating trust for networking services. It requires data collection from various sources: physical & local data sources.
- The trust evaluation procedure is fed by the following inputs.
  - Pre-provisioned or manually configured by policy or management information
  - Analysis from interactions between autonomic nodes
  - The accumulated history information of trust verifications such as authentication of non-autonomic nodes and validity of application specific transactions.
  - other unaccepted or unexpected behaviors
- Trust evaluation procedure between autonomic nodes at same trust networking domain are taken for trust identification
- More specifics of trust evaluation mechanism is for further study

TN Procedures: Node Registration

(1) Node A connects to the network of trust networking domain;

(2) The domain assigns a private IP address to Node A. The domain gateway is assigned as the default gateway for IP network;

(3) Trust information management ASA analyses the trust information of node A;

(4) Node A request to join the domain;

(5) Domain membership management ASA of the domain administrator receives the requests and decides to approve Node A, based on the domain policy and trust level of Node A;

(6) ID-Location management ASA of the domain administrator issues a new identifier of Node A;

(7) ID-Location management ASA archives Node A’s identifier and private IP address.

```
+-----------+          +-------------+    +----------------+
|           |   (1)    |             |    |                |
|           +---------->  Domain     |    |                |
|           |   (2)    |  Gateway    |    |  Trust Info.   <---+
|           <----------+             |    |  Management    |   |
|           |   (3)    +-------------+    |     ASA        |   |
|           <-----------------------------+                |   |
|           |                             +----------------+(5)|
|           |                             +----------------+   |
|           |              (4)            |                |   |
|   Node A  +-----------------------------+ Domain Member  <---+
|           |                             |  Management    <---+
|           |                             |     ASA        |   |
|           |                             +----------------+   |
|           |                             +----------------+(7)|
|           |                             |                |   |
|           |              (6)            |  ID-Location   |   |
|           <-----------------------------+  Management    <---+
|           |                             |     ASA        |
+-----------+                             +----------------+
```

TN Procedures: Communication between TNDs

(1) Host 2 requests IP address of Host 1 to the domain administration ASA 2 through the ID of the host 1;

(2) The domain administration ASA 2 requests IP address of the Host 1 to the domain administration ASA 1;

(3) The domain administration ASA 1 obtains IP address of the Host 1 and reply ID and IP address of the Host 1 to domain administration ASA 2, and it replies to Host 2;

(4) Host 2 requests a trust level of Host 1 through the domain administration ASA 2;

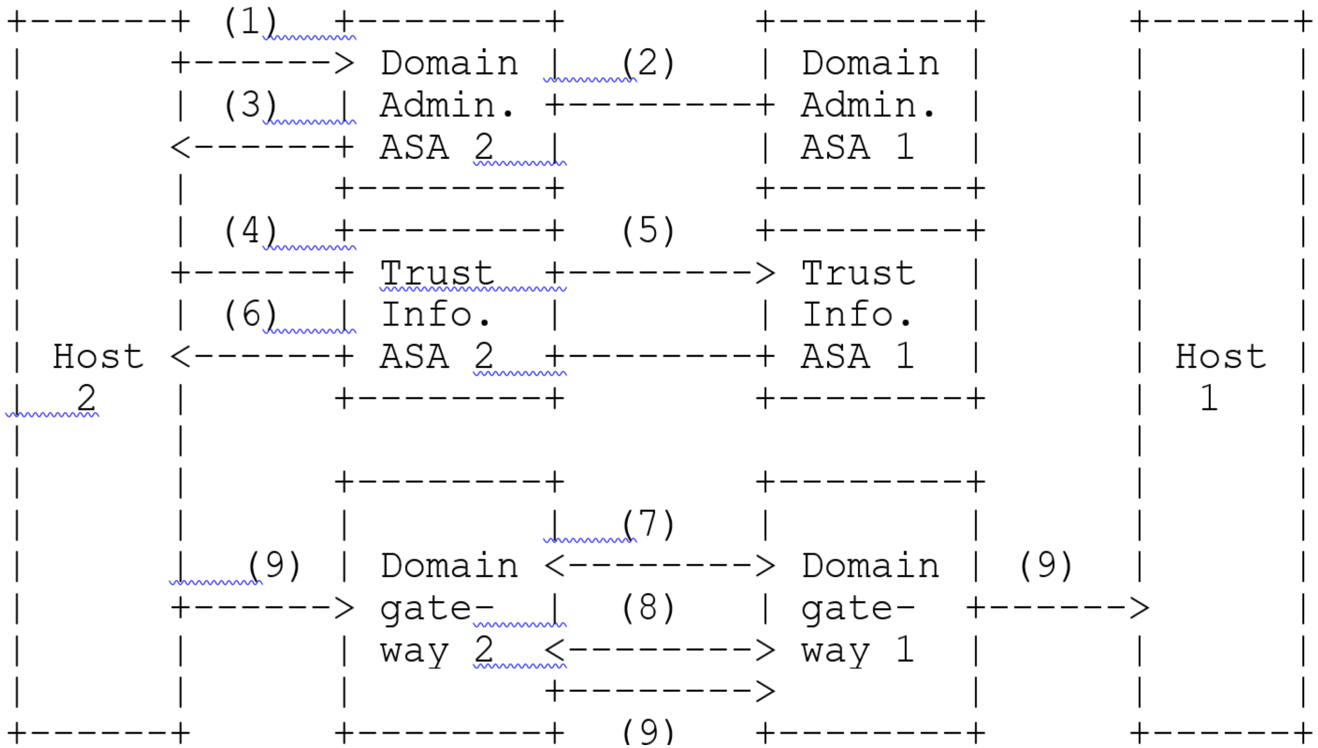
(5) The domain administration ASA 2 checks a trust level of Host 2 through the trust information management ASA and requests a trust level of Host 1 to domain administration ASA 1;

(6) The domain administration function 1 obtains the trust level of Host 1 through the trust information management ASA and replies it to the domain administration ASA 2, and the result replies to Host 2;

(7) The domain gateway ASA 2 forms a routing path with the access and delivery control function 1 through the ID-based routing ASA;

(8) The Host 2 and the Host 1 establish a reliable link through the domain gateway ASA of each trust networking domain;

(9) Networking path established between Host 1 and Host 2.



```
+-------+ (1)  +---------+         +---------+      +-------+
|       +------> Domain  |   (2)   | Domain  |      |       |
|       | (3)  | Admin.  +---------+ Admin.  |      |       |
|       <------+ ASA 2   |         | ASA 1   |      |       |
|       |      +---------+         +---------+      |       |
|       | (4)  +---------+   (5)   +---------+      |       |
|       +------+ Trust   +---------> Trust   |      |       |
|       | (6)  | Info.   |         | Info.   |      |       |
| Host  <------+ ASA 2   +---------+ ASA 1   |      | Host  |
|  2    |      +---------+         +---------+      |  1    |
|       |                                           |       |
|       |      +---------+         +---------+      |       |
|       |      |         |   (7)   |         |      |       |
|       |  (9) | Domain  <---------> Domain  | (9)  |       |
|       +------> gate-   |   (8)   | gate-   +------>       |
|       |      | way 2   <---------> way 1   |      |       |
|       |      |         +--------->         |      |       |
+-------+      +---------+   (9)   +---------+      +-------+
```