IKEv2/IPsec Context Definition

draft-plmrs-ipsecme-ipsec-ikev2-context-definition-00

Daniel Palomares, Orange Labs – LIP6

Daniel Migault, Orange Labs

INTRODUCTION

- Motivation:
  - Large clusters may take advantage: fail-over with high availability, load-balancing, scalability of overloaded SGs, etc.
  - For security reasons, operators are interested in vendors interoperability for clustering IPsec platforms.
- Current standard:
  - RFC6311 adds protocol support for High Availability (counters).
  - RFC6027 IPsec Cluster Problem Statement
  - Today, IKEv2/IPsec parameters synchronization is application specific.
- Goal of the document:
  - To list the IKEv2/IPsec parameters and their associated level.
  - This draft does not define format for the parameters/context.

IKEv2 Session Keys

- Case 1:
  - The node sends the private Diffie-Hellman key, the peer's KE content and nonces.

- Case 2:
  - The node sends the SKEYSEED and nonces.

- Case 3:
  - The cluster memeber sends all computed keys
  - SK_* = SK_d, SK_ai, SK_ar, SK_ei, SK_er, SK_pi, SK_pr).

- SKEYSEED and its derivatives are computed as follows:
  - SKEYSEED = prf(Ni | Nr, g^ir)
  - {SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr } = prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr)

IKEv2 Parameters Definition

MANDATORY

IKE Version
INITIATOR and RESPONDER flags
Local/Remote host address (IPv4 or IPv6)
INITIATOR's and RESPONDER's IKE_SA SPI
Incoming/Outgoing Message IDs
The cryptographic material for the IKE_SA
[SA]Proposal enc r/int algos and key length, prf
Extensions and Condition of the IKE_SA (NAT, EAP, MOBIKE...)
IDi/IDr (ID_IPV4_ADDR, ID_IPV6_ADDR, ID_FQDN, etc.)
Credentials (pre-shared keys or digital certificates)
The Windows bitmap

VENDOR SPECIFIC

n/a

OPTIONAL

IKE lifetime
Vendors ID

IPsec Parameters Definition

MANDATORY

Local/Remote host addresses (IPv4 or IPv6)
Inbound/Outbound IPsec_SA SPI
IPcomp flag, CPI-CPO, IPcomp algo
SN counters and SN overflow flag
Incoming/Outgoing Message IDs
The anti-replay window value.
IPsec mode: transport or tunnel mode
The SA Lifetime
Path MTU: maximum size of an IPsec packet that can be transmitted without fragmentation.
Upperspec: upper-layer protocol to be used.
Source IP/Destination IP addresses and ports of the protected traffic.
ESP - AH encryption/integrity algorithms and key lengths.
The crypto material: KEYMAT (encryption and/or authentication keys).

VENDOR SPECIFIC

Instance-id or flow-id: it helps a node to identify which packet processing unit will process this ipsec traffic or which ipsec instance out of multiple ipsec processing units will process this ipsec traffic.

OPTIONAL

n/a

COMMENTS

- Version -01: (comments from the mailing list)
  - Intended status: INFORMATIONAL.
  - Explicitly include some parameters (message IDs, IKE lifetimes, etc.).
  - Should the SG send only computed keys SK_*?
    - Or instead: DH Secret + nonces + keys.
  - Define different levels within the context:
    - **Mandatory – Optional – Vendor Specific**

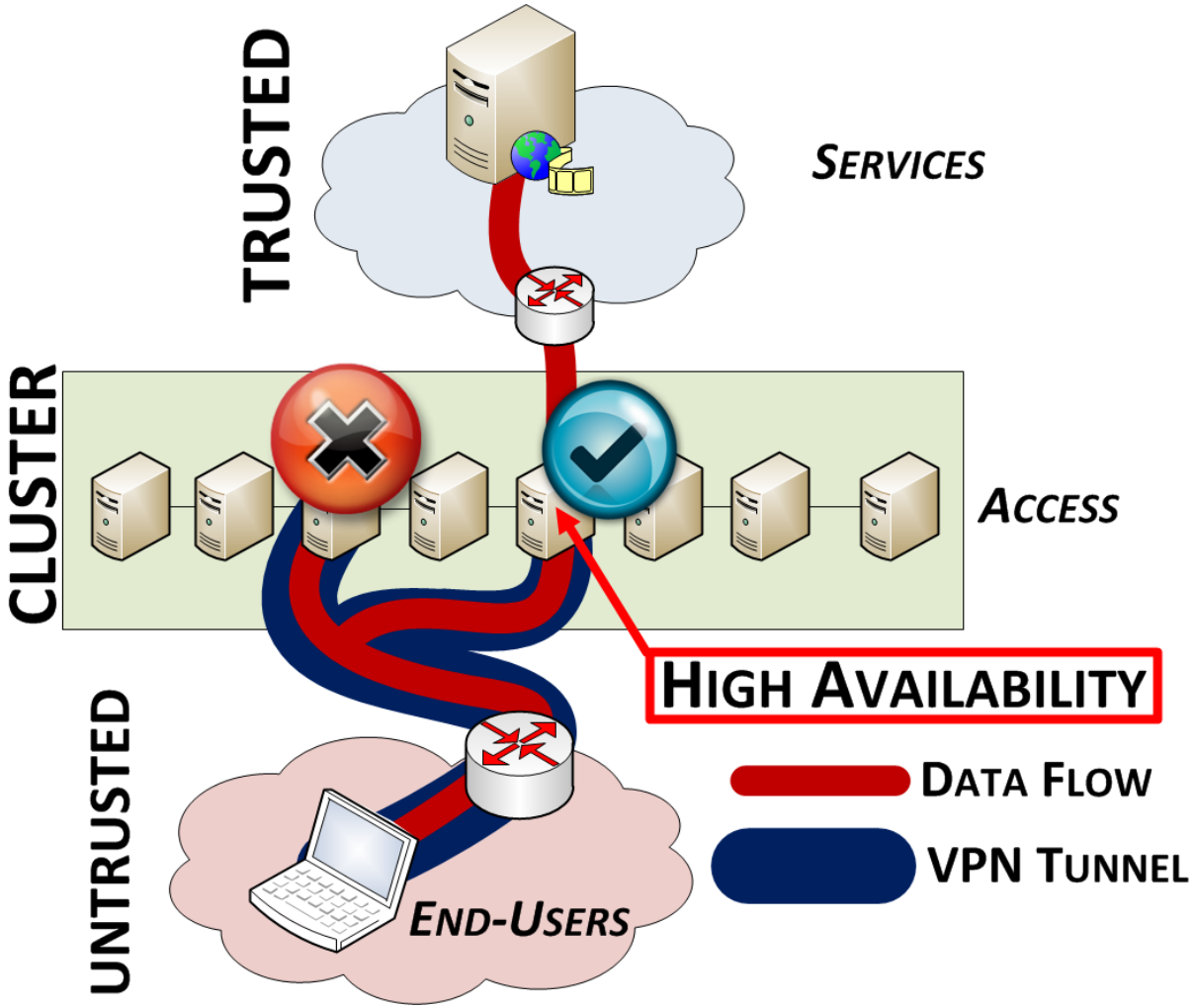
CONCLUSIONS

- Comment on

<draft-plmrs-ipsecme-ipsec-ikev2-context-definition>

QUESTIONS

HIGH AVAILABILITY



TRAFFIC MANAGEMENT