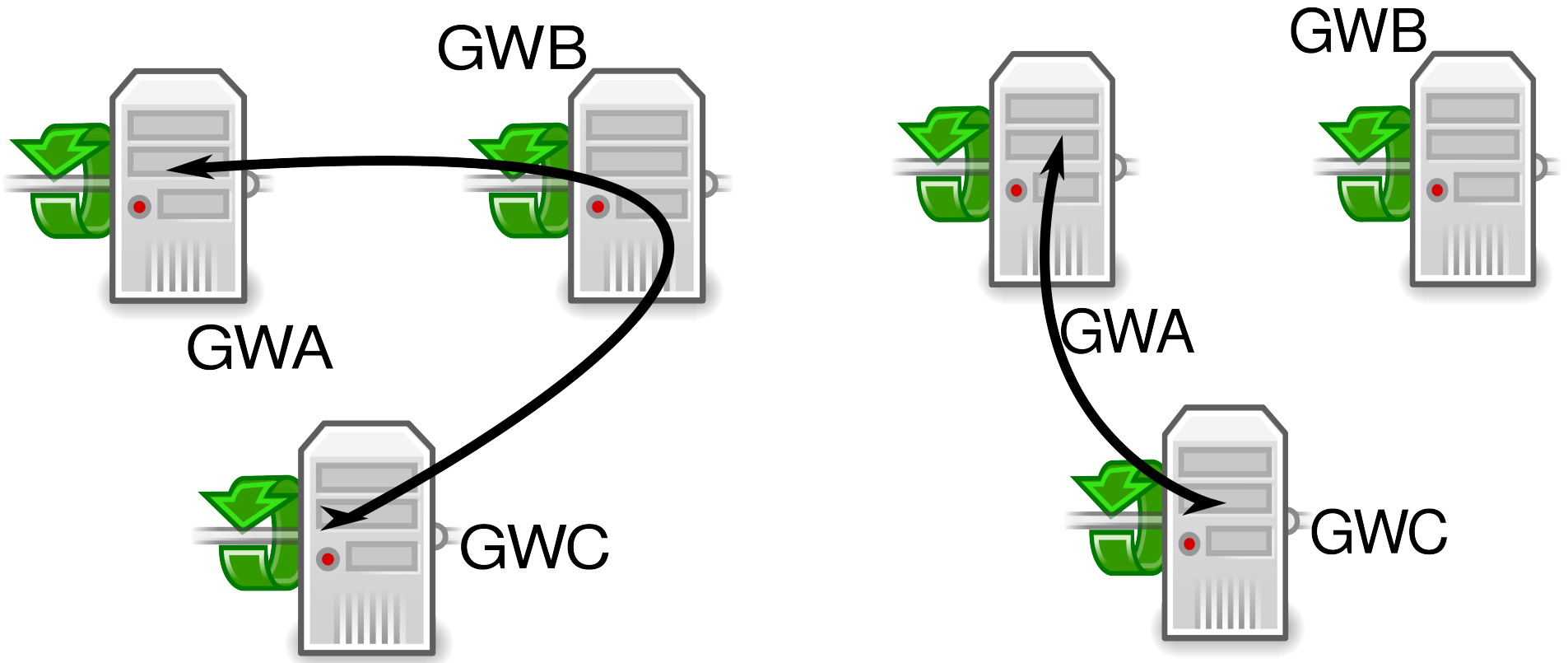
Auto Discovery VPN Protocol

draft-sathyanarayan-ipsecme-advpn-03

Auto Discovery VPN Protocol

- A solution proposal for the AD-VPN problem statement.
- Active document:
  - -00 version submitted 5-July presented in Berlin
  - -01 version submitted on 21 august
  - -02 version submitted on 09-september
  - -03 version submitted on 21-october
- 48 pages
- Based on “shortcuts”:
  - If gateway C decrypts traffic from A, re-encrypts it and sends it to B, then C can tell A and B to communicate directly.

Auto Discovery VPN Protocol in one Slide



If gateway A decrypts traffic from A, re-encrypts it and sends it to C, then B can tell A and B to communicate directly with a SHORTCUT

Auto Discovery VPN Protocol - Detailled

- ADVPN single exchange between Shortcut Suggester and Shortcut partners is:

HDR, SK {IDa, ADVPN_INFO, IDi,

IDr[, TSi][, TSr][, VID]} -->

<== HDR, SK

{N(ADVPN_STATUS)}

Questions & Answers

- NAT?
  - YES:
  - Except when peers in different networks have the same address plan. 192.168.1.1 from network A cannot establish a SHORTCUT with 192.168.1.1 in network C
  - Except establishing shortcut between NATed VPN.
  - This case is left for future extensions [draft-brunner-ikev2-mediation-00]
- Can authentication rely on a single administrative domain defined by a certificate instead of PSK?
  - YES: IDi/r are provided for certificate match

Our solution's Pros

- The ADVPN Protocol is an extension of IKEv2 [RFC5996]
  - It does not require additional protocols (e.g. GRE+NHRP+Routing Protocol)
  - It does not rely on routing protocols, thus match them all.
  - SHORTCUT request provisioning are performed in one round trip.
  - SHORTCUT establishment is an IKEv2 4-packet exchanged.

Strength of our solution

- Less centralized, lighter configuration (HTTPS)
  - Static data as long as we don't add subnets
  - GRE Tunnels and subnets have to be configured
  - mao-draft needs to configure the ADS with a lot of informations
- ADVPN provides intra-domain (certificate) and inter-domain authentication

Proposal Comparison

All solutions match ADVPN requirements in different ways:

- Our ADVPN is an IKEv2 Extension solution
  - Only cares about IPsec configuration
  - Uses IPsec built-in tunneling/routing facilities
  - Routing topology is not in the scope of ADVPN, but left to routing stacks.
- DMVPN is a routing architecture:
  - NHRP/Routing Protocol are used to set routing tables
  - GRE Tunnels carry data. IPsec secures GRE tunnels
- ADVPN2 is between DMVPN and ADVPN
  - Uses IPsec Tunnel facilities
  - Routing centric with ADS
  - Uses a specific protocol for its settings.

RFC 7018 Requirements, ditto for p. 11-14

- Req 1, 2: Minimal changes
  - Basically the same for all propositions
  - DMVPN and ADVPN2 rely on more centralized solutions, (NHRP Server ADS)
  - ADVPN is more gateway-to-gateway
  - Note DMVPN uses GRE/IPsec
- Req 3: Proposals enable additional routing/GRE
  - ADVPN provides the IPsec framework for **all** routing applications
  - ADVPN2 and DMVPN are routing based architectures

RFC 7018 Requirements, ditto for p. 11-14

- Req 4:
  - OK for all propositions
- Req 5:
  - ADVPN uses IKEv2 for authentication, and can use ephemeral authentication credentials (PSK).

RFC 7018 Requirements, ditto for p. 11-14

- Req 6:
  - ADVPN performs roaming using MOBIKE and only interacts with the attached SG
  - DMVPN and ADVPN2 use alternate protocols (e.g with the ADS).
- Req 7:
  - None of the proposals uses IPsec based mechanisms to load balance the traffic between SG.
  - ADVPN MAY use cluster IP based solutions, or IPsec context transfer based solutions.

RFC 7018 Requirements, ditto for p. 11-14

- Req 8:
  - ADVPN handles NAT and uses NAT detection mechanisms provided by IPsec.
  - Double NAT with equal address space is not handled by ADVPN, nor by other proposals.
- Req 9: OK
- Req 10:
  - ADVPN enables different organization to merge at the IPsec level, that is providing ephemeral credentials.
  - Routing issues are left to other protocols.
  - ADVPN2 and DMVPN deal with routing issues too.

RFC 7018 Requirements, ditto for p. 11-14

- Req 11, 12, 13? 14: OK
- Req 15:
  - QoS enforcement is performed at different layers.
- Req 16:
  - ADVPN does not have single point of failure
  - ADS MUST have additional mechanisms to avoid being single point of failures

ADVPN

Thanks!

Auto Discovery VPN Protocol - Detailed

- A, B, and C are three spokes, gateways, terminal nodes:
- Support of ADVPN is performed with ADVPN_SUPPORTED Notify Payload
- B estimates a SHORTCUT between A and C would reduce its load for example.
- B becomes a **Suggester** and designates A as **Shortcut Initiator** and C as a **Shortcut Responder**.
-

Auto Discovery VPN Protocol - Detailed

- B sends A and C an ADVPN_INFO Payload providing the necessary information to reach and establish the IPsec/IKEv2 SAs
  - ADVPN_INFO provides:
    - Shortcut ID
    - Lifetime
    - Role: Shortcut Initiator/Shortcut responder
    - PSK
    - Peer Port (NAT)
    - Peer Description
  - IDa the IP address used to reach the Shortcut partner (partner IP address / NAT public IP address)
  - IDi/r to use during the IKE_AUTH exchange
  - TSi/r to negotiate the SA

Auto Discovery VPN Protocol - Detailed

- A and C establish their SHORTCUT
- A and C report the Suggester (B) the status of the SHORTCUT with an ADVPN_STATUS Payload.