draft-saumvinayak-bess-all-df-bum

Saumya Dikshit

Vinayak Joshi

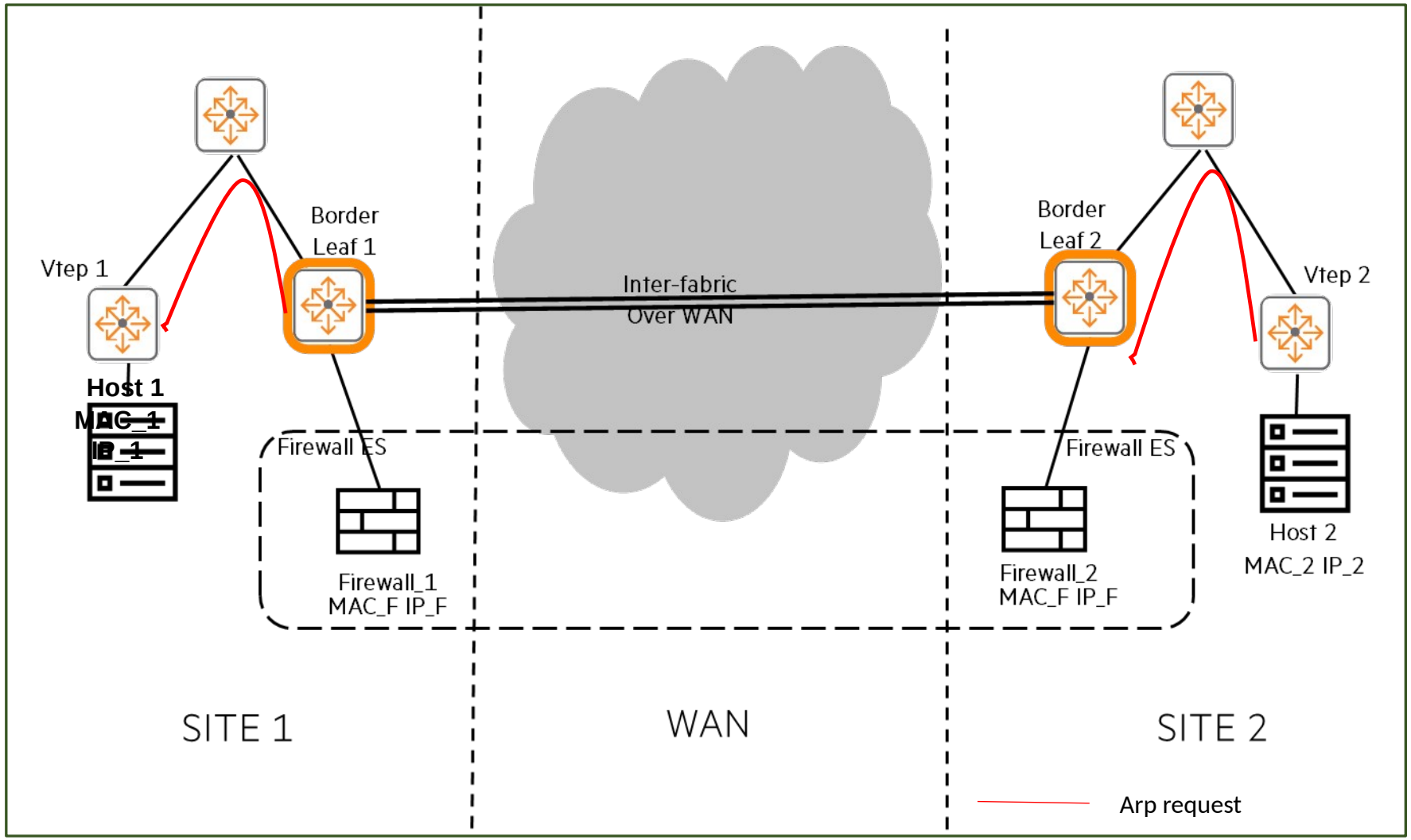
Agenda

- Introduction
- Problem Statement and Use-Case
- Solution
- Inter-operability and Backward Compatibility

Introduction

- Curious case of managing
  - Physical devices (placed across WAN) with same credentials (IP/MAC)
  - Attached to the same Ethernet Segment (ES) of the NVO fabric
- Active/Active Firewall Deployments support redundancy across networks/fabrics
  - Deployed in disparate network
  - Local firewall chosen lest an outage
- Control plane need to respond/align accordingly
  - To ensure desired data plane flows are directed towards local

Problem Description: Distributed Firewall over same Ethernet Segment and EVI cont…..



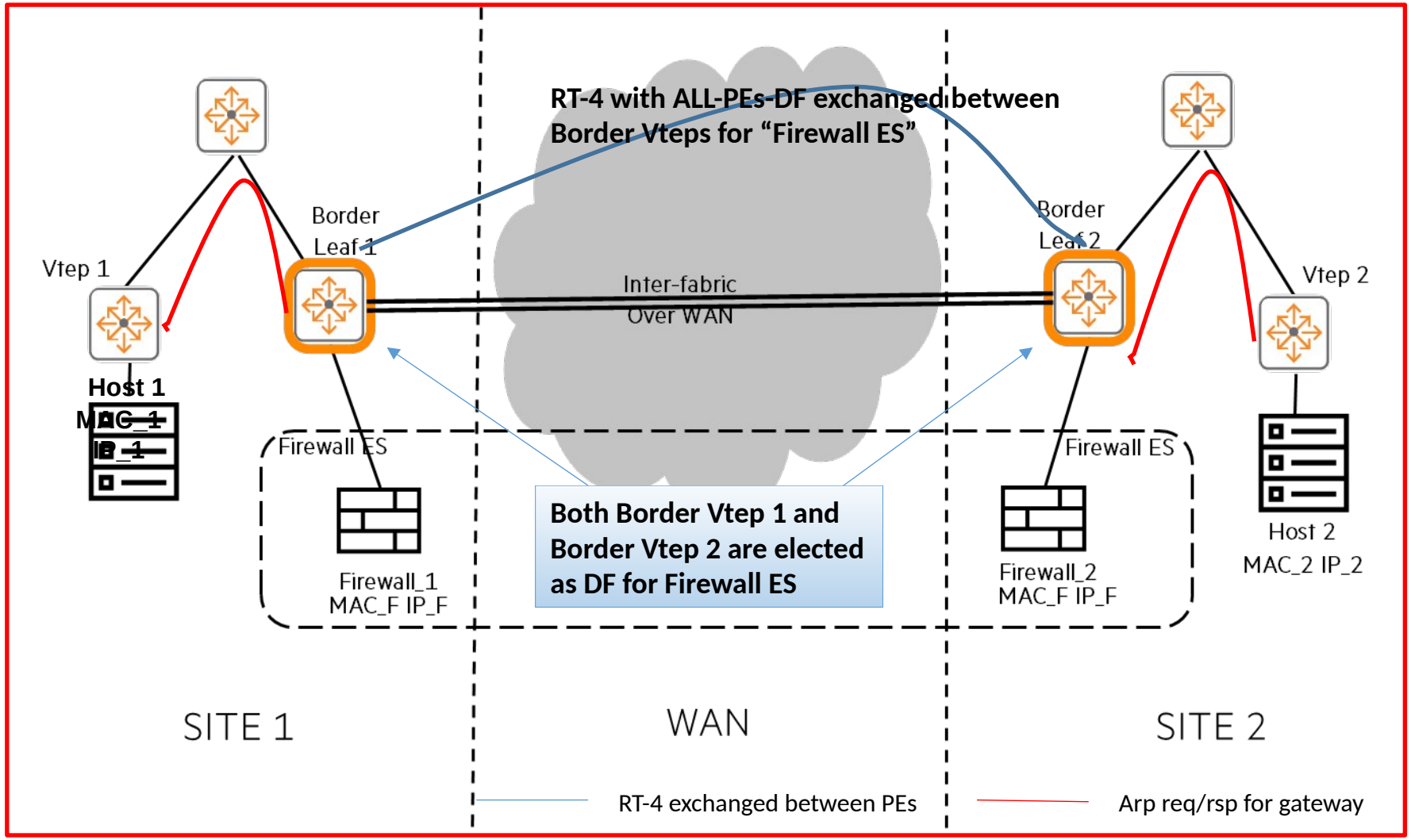
Problem Summary:

- It's a case where PEs (Border Vteps) are in **disparate networks fabrics/sites** and
- the AC's (mapped to **same ES**) behind PEs are not connected to a common physical device (but to **more than one physical device** carrying same credentials).

Problem Description: Distributed Firewall over same Ethernet Segment and EVI

- Two Vxlan sites, **SITE-1 and SITE-2**
  - hooked over **WAN** via Border Vteps.
- Border Vteps configured
  - **with same Ethernet Segment (Firewall ES)** over Firewall Vlan (ESI).
  - One Firewall for each site, with same virtual credentials (MAC_F, IP_F)
- Traffic (including BUM) generated by Host1 (in SITE-1), over **Firewall Vlan**,
  - should run through **site-local firewall** (firewall_1) **preferably**.
- Only **in case of local-outage**,
  - the traffic should be send across over WAN to the remote firewall (firewall_2).
- **Same should apply to traffic generated by Host2 (in SITE-2),**
  - wherein, it should preferably run through the local firewall (firewall_2) and
  - over a failure should go over the WAN towards firewall_1.
- **Both Border Vteps to need to act as Active DFs.**
  - N**ot possible with current standards** ??
- **For example**,
  - Any **ARP request** for firewall credentials landing at either Border Vtep1 or Border Vtep2
  - should be **flooded ONLY to network towards the local firewall**.

Solution: All-PE-DFs mode for DF-election cont….



Solution Summary:

- **new mode of DF-election, ALL-PEs-DF**
- where-in **all of the pariticipating PEs intend to play DF role** for a vlan(s) enabled on the ES
- requires "DF Election Extended Community" to carry this information with the ES route to indicate it to remote PEs
- For example, **Border-Vteps** indulge in publishing ALL-PEs-DF mode for "Firewall ES" in EVPN Route Type-4, thus concluding both are DFs in the Segment.

Solution: All-PE-DFs mode for DF-election cont….

SEND SIDE PROCESSING

The All-PEs-DF mode is used as follows:

- PEs configured to use ALL-PEs-DF mode SHOULD set "DF Alg“ algorithm field in 'DF Election Extended Community' to appropriate value.
- This document proposes value '2' for All-PEs-DF mode, as values '0' and '1' are already defined for usage in [RFC8584].
- This algorithm is agnostic to the values carried in 'Bitmap' but does not discounts any use-case(s) in future which may need extra information carried in 'Bitmap' along with All-PEs-DFmode.

Receive SIDE PROCESSING

The All-PEs-DF mode is used as follows:

- PE receives the ES routes from all the other PEs for the ES in question carrying the ALL-PEs-DF mode set in 'DF Election Extended Community', it SHOULD checks to see if all the advertisements have the Extended Community with 'All-DF-mode' set as 'DF Alg'.
- If yes, then SHOULD ignore the 'Bitmap' and 'Rsvd' field in the extended community.
- As also mentioned in [RFC8584] , if even a single advertisement for Route Type 4 is received without the locally configured DF Alg and capability, the default DF election algorithm MUST be used as prescribed in [RFC7432].

Interoperability and Backward Compatibility

- RFC7432 rules applicable.

Request to the Bess Group

- To Discuss this and add this as a WG draft.
- Please point to any existing work on the same lines which solves this problem.