envoycon NORTH AMERICA

Dynamic Configuration and Scaling of VPN Concentrator and Envoy SASE Proxy in Multi-Tenant Edge

Srinivasa Addepalli & Ritu Sood, Aryaka
Mrittika Ganguli, Jeff Shaw, Intel Corporation

envoycon
NORTH AMERICA

November 12, 2024
Salt Lake City

Srinivasa Addepalli
CTO
Aryaka

Ritu Sood
Distinguished Engineer
Aryaka

Mrittika Ganguli
Principal Engineer
Intel Corporation

Jeff Shaw
Software Architect
Intel Corporation

Demo, benchmarks:
Abhirupa Layek, Network Engineer, Intel

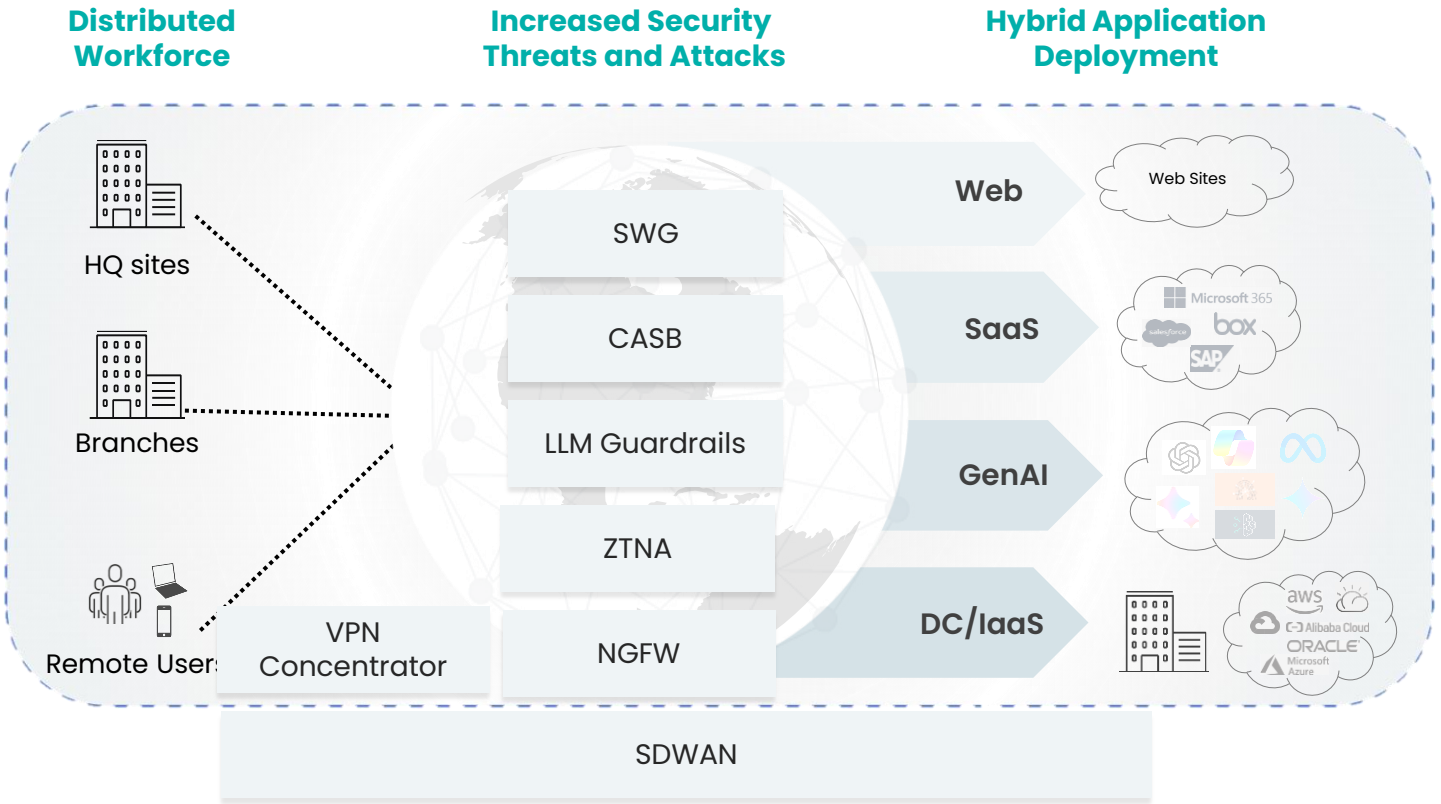
Introduction

envoycon NORTH AMERICA

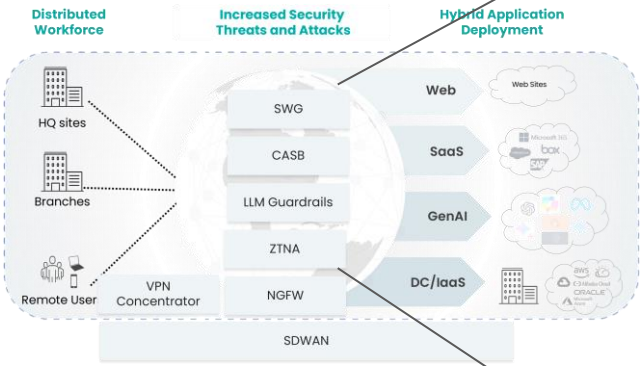
- What is SASE/SSE?
  - The need for a proxy in SASE/SSE.
  - Why Envoy is the right choice for a proxy.
  - Enhancements made to optimize Envoy for SASE/SSE.
  - The role of VPN concentrators in SASE/SSE.
  - Why single-tunnel throughput performance is crucial.
  - The need for VPP-based IPsec.
  - Essential VPN concentrator functionalities beyond IKEv2/IPsec.
  - Performance metrics and a demo.

  Q&A

Introduction – SASE/SSE for Modern Enterprises



SASE/SSE Security requires Proxy technology



Security Functions

- *Context based Access Controls*
- *URL filtering*
- *Content filtering*
- *DLP*
- *Anti-Malware*
- *LLM firewall*
- *API Firewall*

Requirements

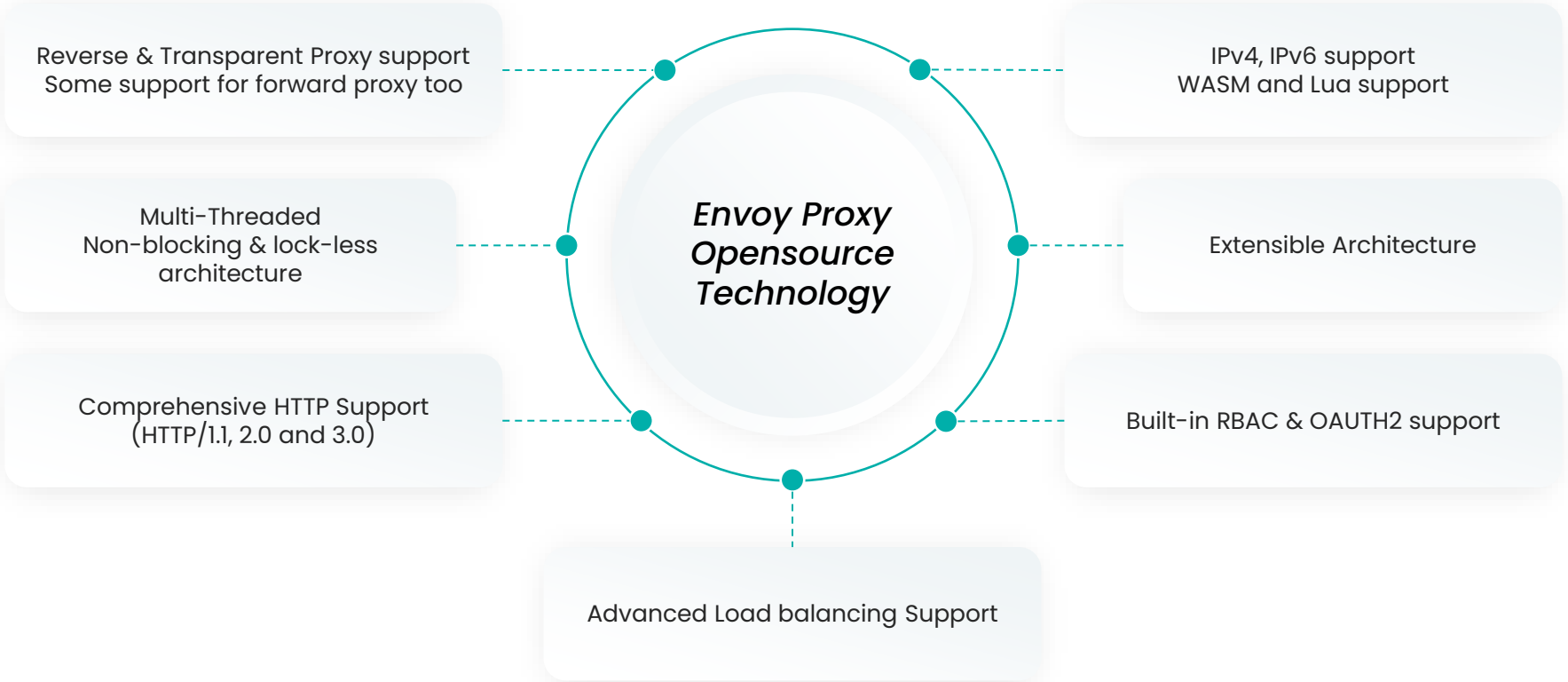
- *SSL/TLS Decryption to get the deeper protocol data.*

- *Termination of TCP*
- *Termination of SSL*
- *Upstream Connection Origination*
- *Mimick Certs*

Proxy technology supporting Forward Reverse and transparent proxy methods

Envoy Proxy for SASE/SSE – Why?

envoycon NORTH AMERICA



What did we do to make Envoy SASE/SSE ready

envoycon NORTH AMERICA

Multi-tenancy
Configuration Isolation
VRF Support
Multi Criteria tenant identification

Rewritten OAUTH filter
(Multiple OIDC clients)

Forward Proxy Authentication
(Kerberos, UN/PWD)

Common Policy Framework
(for multiple functions, Objects support)

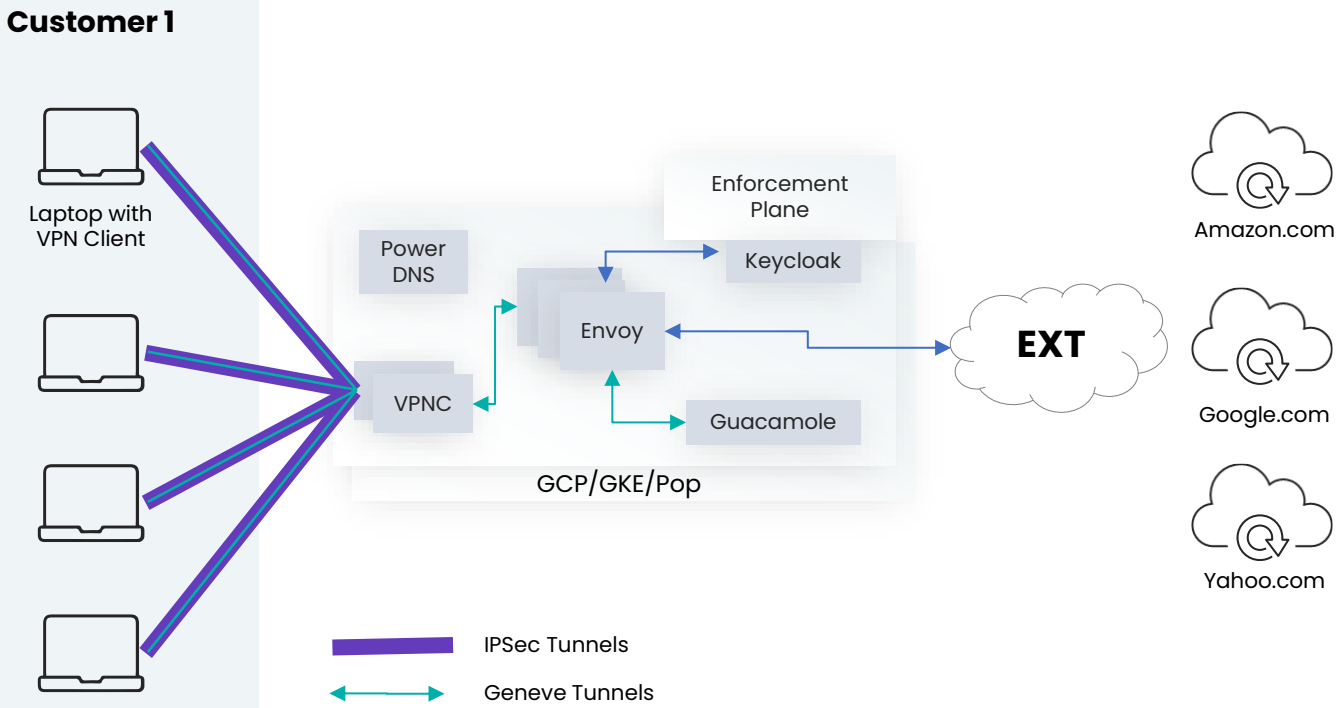
Beyond foundational changes, many security functions as filters

Forward Proxy Authentication
(Kerberos, UN/PWD, Recycling)

Configuration Reuse across multiple listeners

MITM TLS Inspection
(Mimic Cert generation)

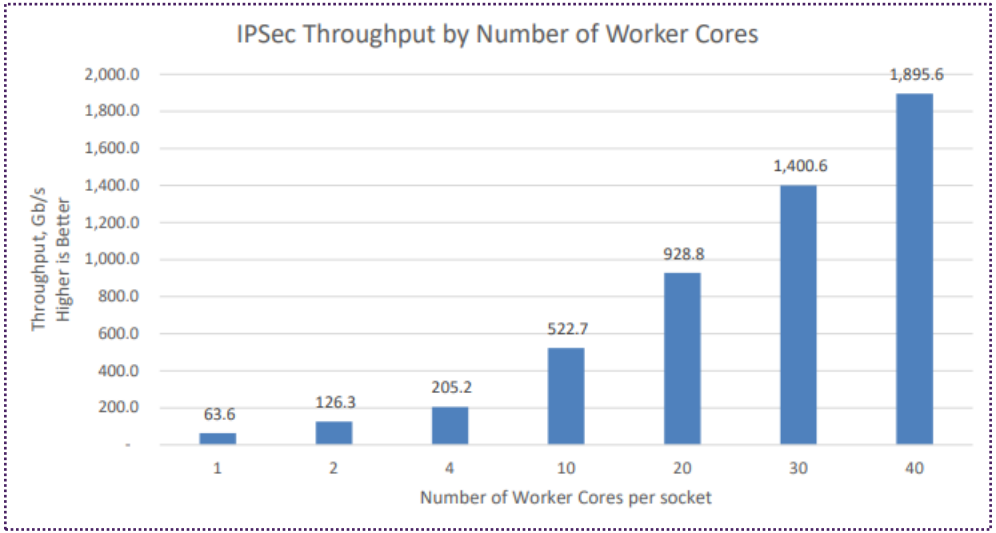
SASE/SSE – Opensource Beyond Envoy



Automation

- Horizontal Pod scaling
  - VPN Tunnels one per tenant location
  - Geneve tunnels one per tenant
  - Internal IP address allocation and routes per tenant per service
- Vertical Scaling

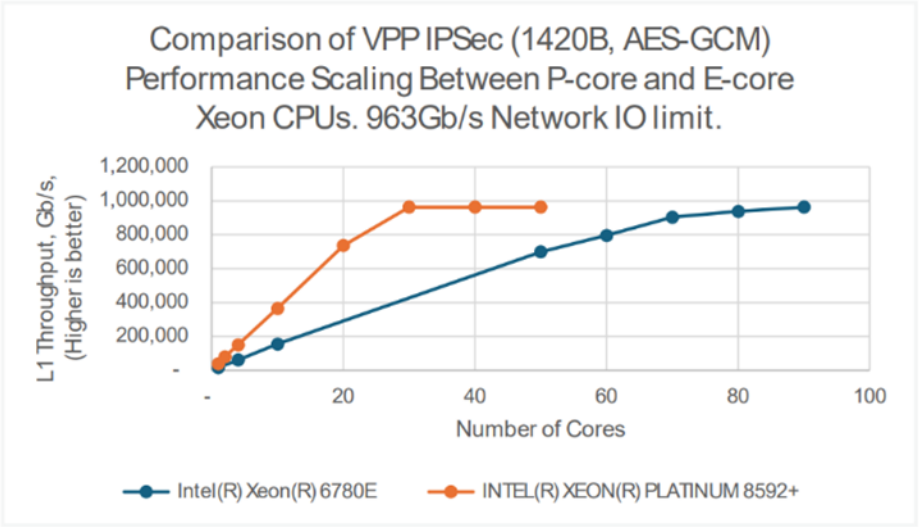
VPP VPNC

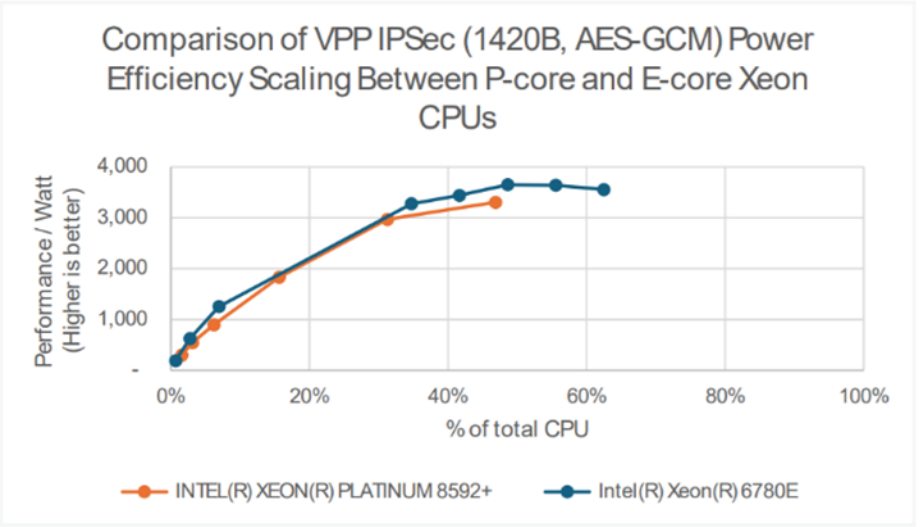


Performance of VPP IPsec Workload Running with Different Number of Worker Cores

Source: Intel® AVX-512 - High Performance IPsec with Intel® Xeon® Scalable Processor
https://networkbuilders.intel.com/docs/networkbuilders/intel-avx-512-high-performance-ipsec-with-intel-xeon-scalable-processor-technology-guide-1683018859.pdf

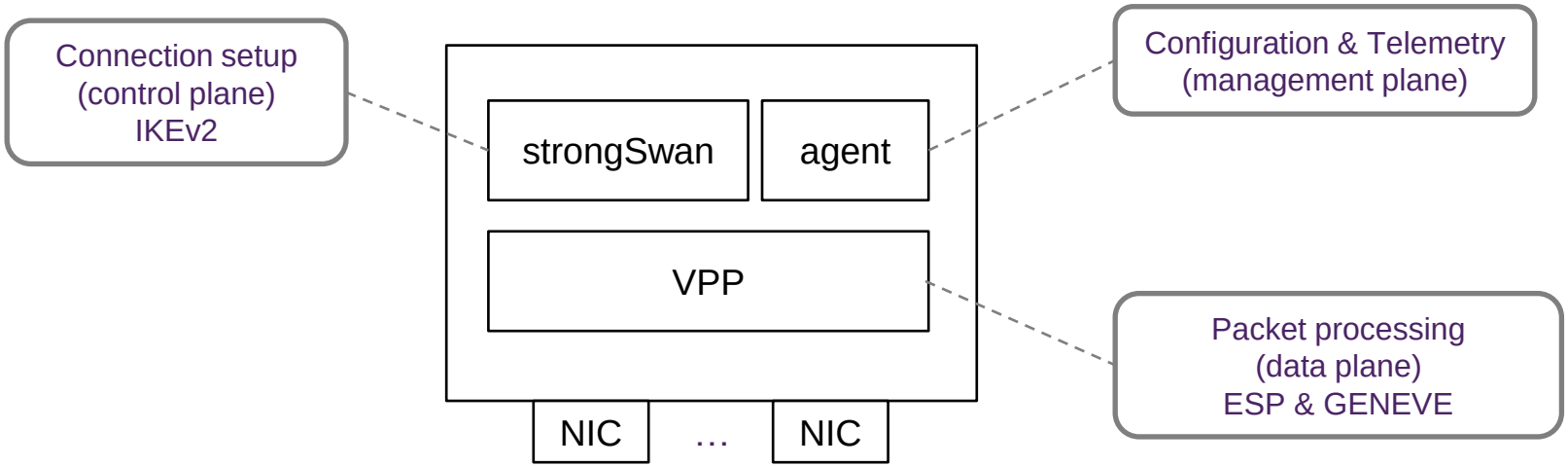
P-core and E-core IPsec scaling





Performance of VPP IPsec Workload Running on different types of CPU

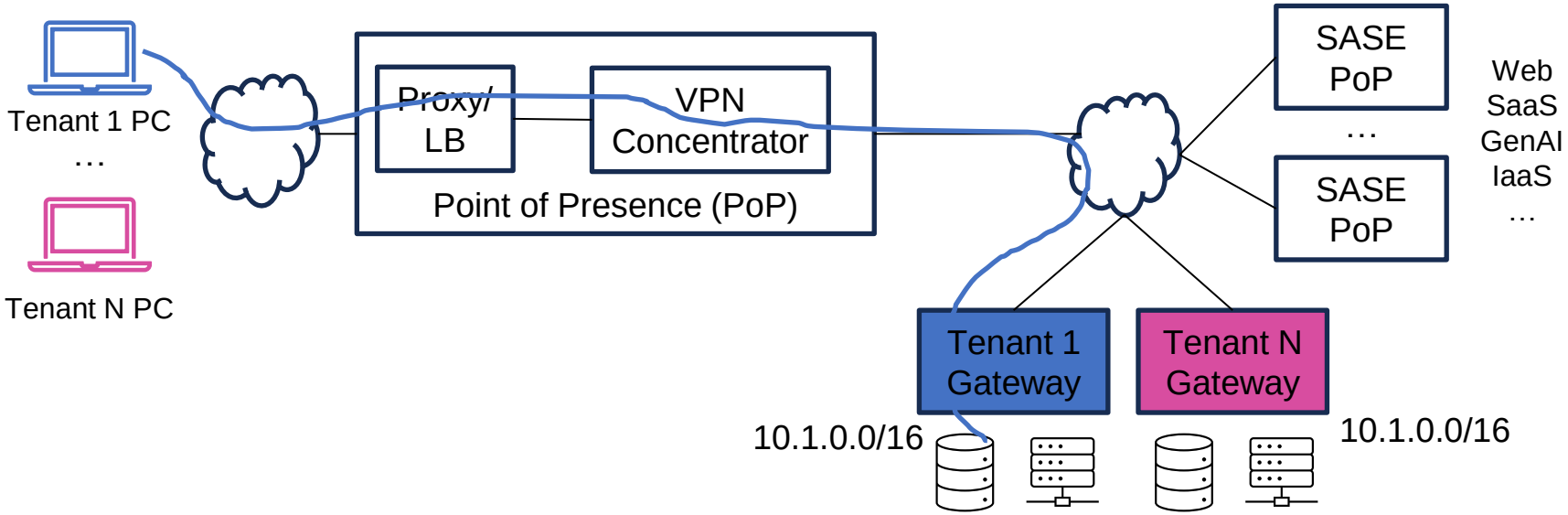
VPP VPNC Architecture



VPP VPNC High Level Architecture

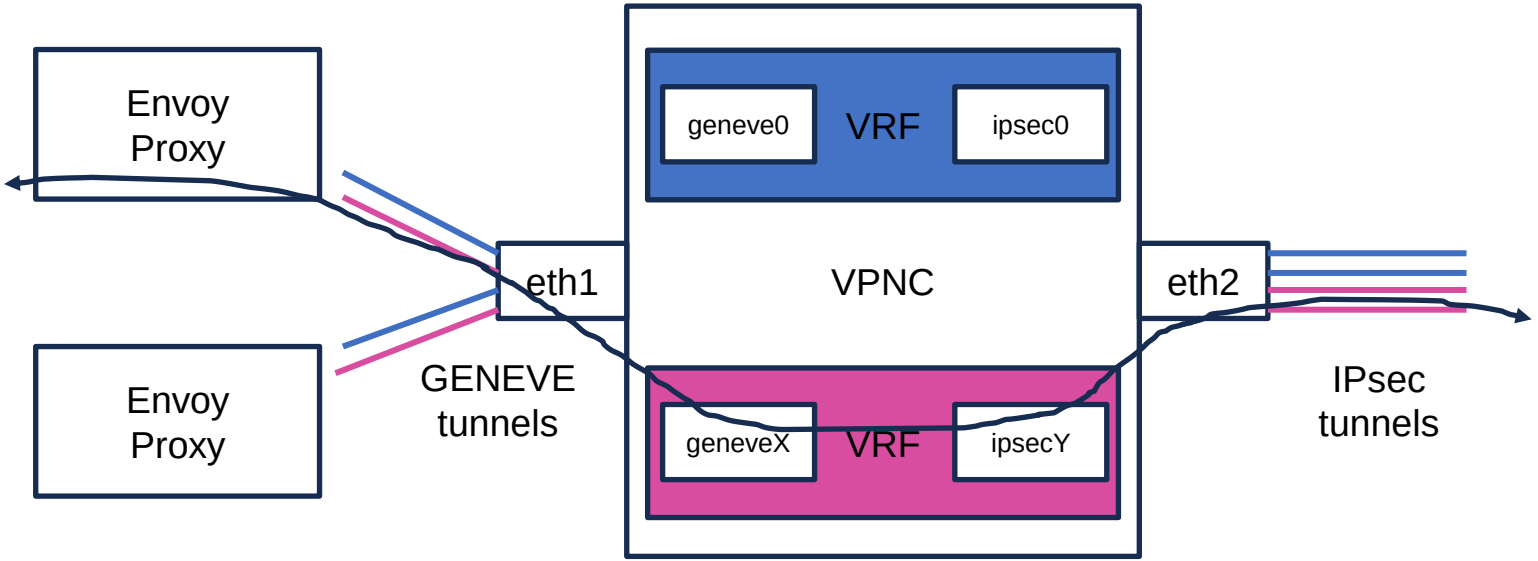
See Whitepaper titled “FD.io VPP-SSwan and Linux-CP – Integrate StrongSwan with World’s First Open Sourced 1.89 Tb IPsec Solution Technology Guide”

Multi Tenancy



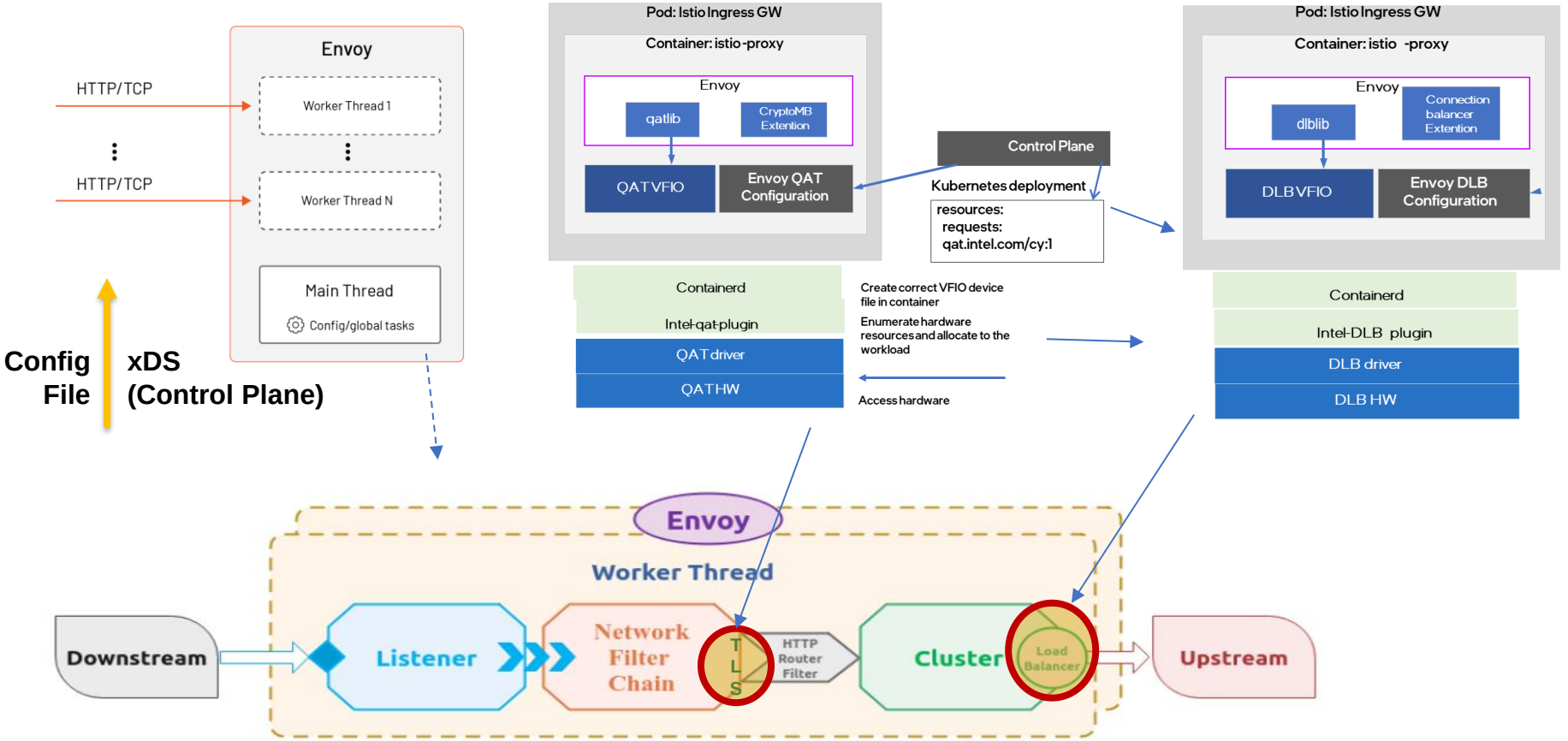
- Need to isolate traffic between tenants
- Tenants have overlapping IP addresses

Multi-Tenant VPNC



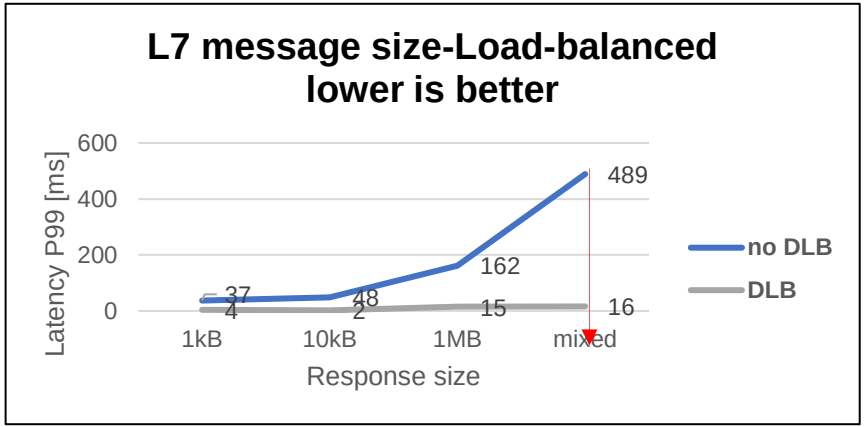
Envoy Acceleration summary

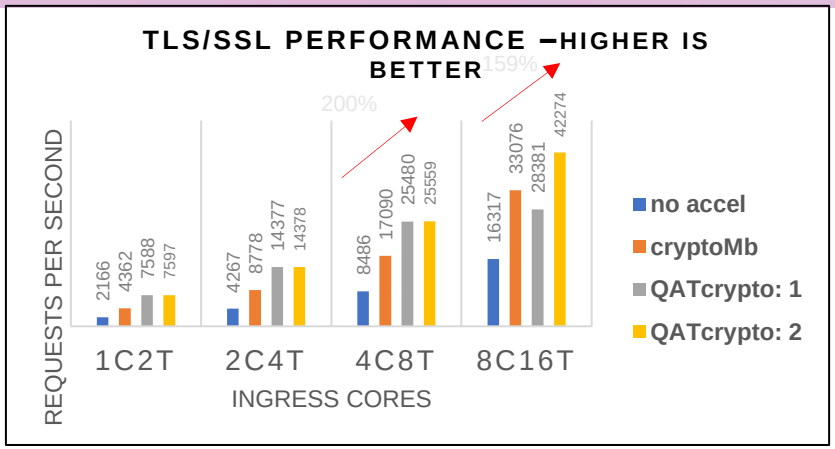
envoycon NORTH AMERICA

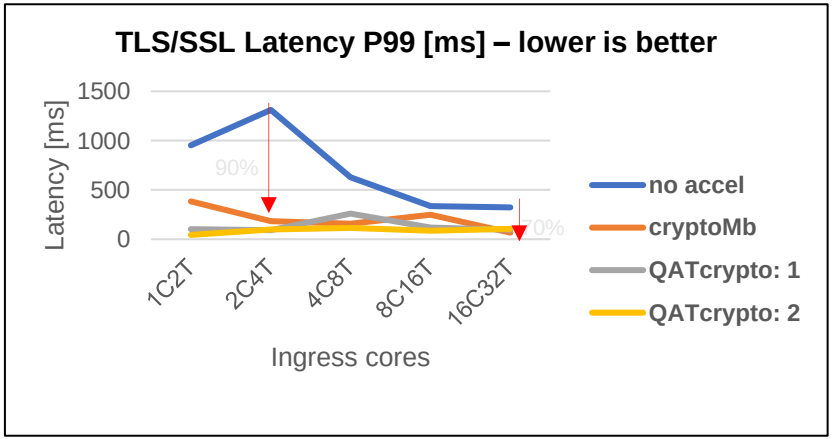


Envoy **Performance** acceleration

envoycon NORTH AMERICA

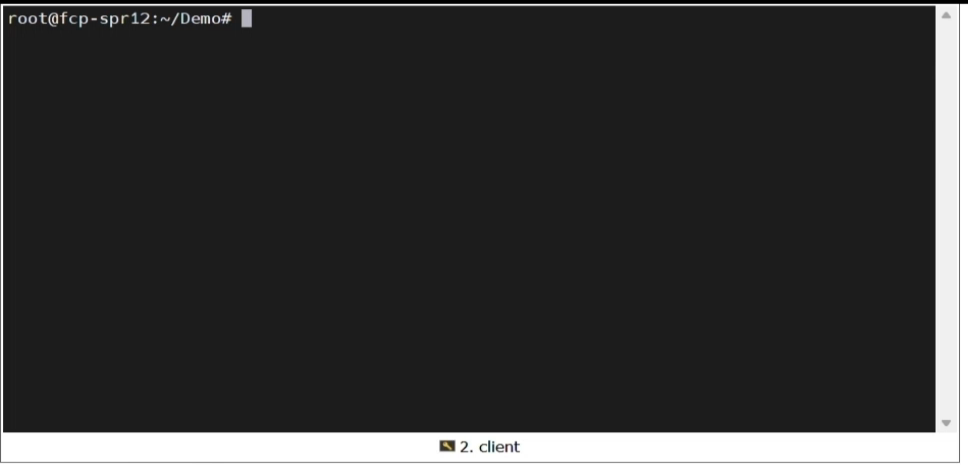


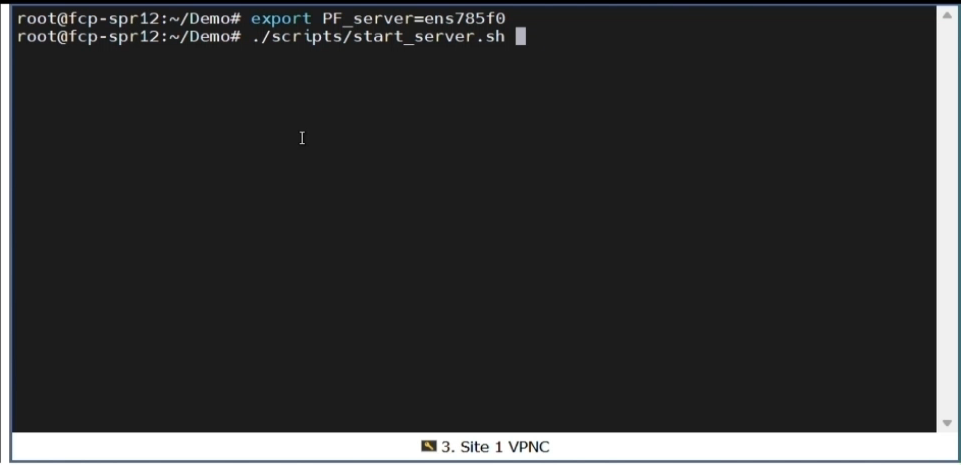


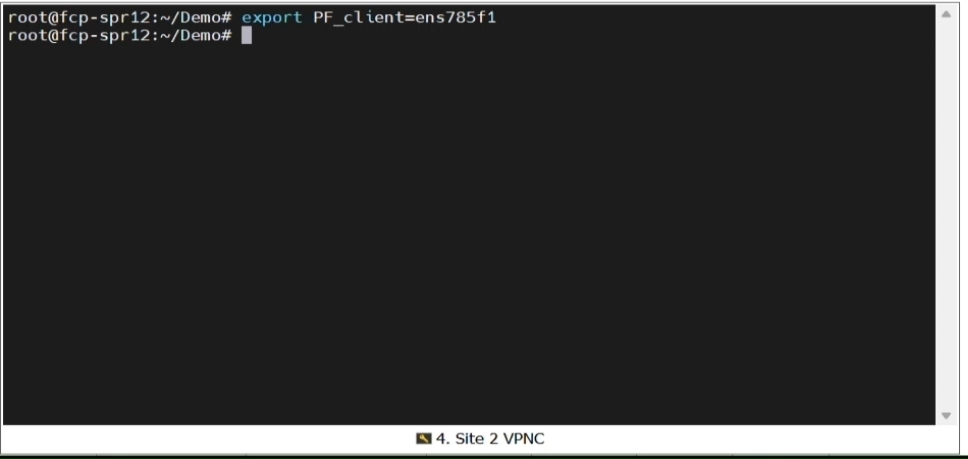


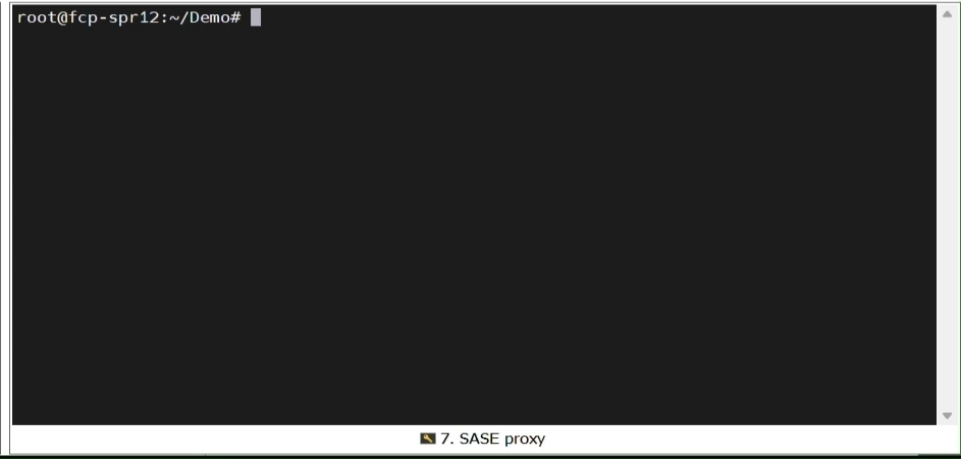
Demo VPNC+Envoy

envoycon NORTH AMERICA









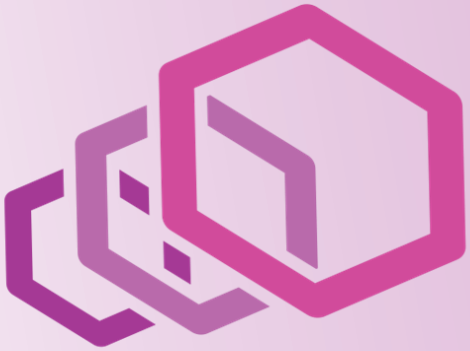
Next Steps

envoycon NORTH AMERICA

- Links:
  - VPP VPNC Whitepaper https://digitallibrary.intel.com/content/digital-library/us/en/assetdetail.html/content/dam/intel-digital-library/audience/business/edge-networking-services-product-brief
  - TLS and load balancing acceleration - https://networkbuilders.intel.com/solutionslibrary/service-mesh-istio-envoy-optimizations-intel-xeon-sp-solution-brief

  - Connect with us for Collaboration

Q&A



envoycon

NORTH AMERICA

Backup

Dynamic Configuration and Scaling of VPN Concentrator and Envoy SASE Proxy in Multi-Tenant Edge

envoycon NORTH AMERICA

Srinivasa Addepalli & Ritu Sood, Aryaka
Mrittika Ganguli & Jeff Shaw, Intel Corporation

This discussion shows a framework that integrates a VPN Concentrator with Envoy-based Secure Access Service Edge (SASE) proxy, leveraging APIs for configuration and management of network functions within containers. This is designed to dynamically scale.

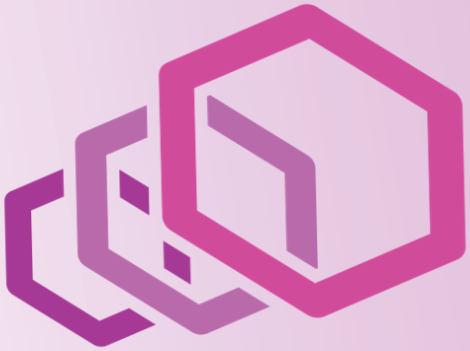
The VPN Concentrator (VPNC) establishes secure IPSec tunnels that encapsulate data traffic, providing privacy and protection against threats. As number of tenants or volume of traffic increases, the need for additional VPNCs, IPSec tunnels and proxies arise.

The SASE proxy is a network filter at the edge, enforcing security policies, optimizing traffic flow, providing a zero-trust network access to cloud-based services. Number of proxies is changed as a ratio-based scaling approach to IPSec tunnels or tenants based on metrics like:

- Throughput, Latency, Error rates
- Active, denied connections
- Security breaches
- Number of active user sessions
- Number of route changes for load-balancing
- Envoy utilization with/without optimization

aryaka

intel



envoycon

NORTH AMERICA

envoycon
NORTH AMERICA

Title

Speaker Name

Title

Content

Title

envoycon
NORTH AMERICA

November 12, 2024
Salt Lake City

Speaker Name
Job Title
Company

Speaker Name
Job Title
Company

Title

envoycon
NORTH AMERICA

November 12, 2024
Salt Lake City

Speaker Name
Job Title
Company

Title

envoycon
NORTH AMERICA

November 12, 2024
Salt Lake City

Speaker Name
Job Title
Company

Speaker Name
Job Title
Company

Speaker Name
Job Title
Company

Speaker Name
Job Title
Company

Speaker Name
Job Title
Company