

Egress Gateway and Core Switch



Overview

Configure interfaces and IP addresses on egress firewalls and core switches. Configure IP addresses for interfaces of FWA, and add the interfaces to security zones.

Key Takeaways

An egress gateway core switch serves as the central point for outbound traffic, managing routing, security, and high availability in both campus networks and Kubernetes environments.

Role in Campus Networks

In traditional campus networks, core switches configured as egress gateways act as the main user gateway and central routing point. They often operate in a cluster switch system (CSS) for high availability, distributing IP addresses to users and connecting aggregation switches to the network backbone. These core switches can integrate with firewalls at the network egress to filter traffic, enforce security policies, and manage NAT for internal and external access.

Features typically include: Hot standby redundancy with paired firewalls for continuous service. Intelligent uplink selection to optimize outbound link usage.

Eth-

Trunk interfaces for link aggregation and reliability. Traffic control policies to restrict certain services (e.g., gaming or streaming) during work hours.

Egress Gateway in Kubernetes

In Kubernetes, an egress gateway provides a stable, fixed IP for outbound pod traffic, which is crucial for integrating with external firewalls or services. The architecture consists of: Control Plane: Manages custom resources, allocates egress IPs, and orchestrates gateway selection. It runs as a Deployment with multiple replicas for high availability.

Data Plane: Enforces policies on each node via DaemonSets, using iptables and VXLAN tunnels to route traffic through designated gateway nodes. Custom Resources: Define policies and egress IP assignments, ensuring that traffic from specific pods, namespaces, or deployments exits through the correct gateway. This setup allows Kubernetes clusters to maintain static egress identities, enabling centralized firewall management, traffic auditing, and secure routing of outbound traffic.

Key Benefits

High Availability: Core switches in CSS or Kubernetes control plane replicas ensure continuous operation. Traffic Management: Dynamic routing, load balancing, and intelligent uplink selection optimize network performance. Security: Integration with firewalls and NAT policies protects internal resources and enforces access control.

Scalability: Supports large-scale deployments in campus networks or dynamic Kubernetes environments. In summary, an egress gateway core switch is a critical network component that centralizes outbound traffic management, enhances security, and ensures reliable connectivity, whether in traditional campus networks or modern containerized environments.

Article Content

Deploying Firewalls as Egress Devices

Configure interfaces and IP addresses on egress firewalls and core switches. Configure IP addresses for interfaces of FWA, and add the interfaces to security zones.

Connecting Firewalls to Egress Routers Directly

At the egress of a large campus network, core switches are directly connected to upstream firewalls and connected to egress gateways through firewalls. Two routers function as

Egress Switch Best Practice and Security Guide v4.x

The following section covers best practice deployment recommendations for the Egress Server Infrastructure, Switch Gateway and Switch Client software. The following guidelines will ensure high

Core Switch vs. Distribution Switch vs. Access Switch

There are different types of enterprise switches that perform various roles in these layer-based or hierarchical ethernet networks. This white paper introduces the following three types of network

Routing on firewall or core switches? : r/networking

In my research I'm getting mixed suggestions - Some say that core switches are for routing, when others say that core switches have to be as fast as possible and have minimal tasks dedicated to them.

Must Gateways Be Configured at the Core? A Complete ...

If you've ever wondered: Can aggregation switches handle VLANIF interfaces? Will using the core as a gateway overburden it? Is it secure to place gateways at the access layer? After

Integrated Routing and Bridging (IRB) Design Models

Access switches perform bridging, and core switches perform routing. The core switches have to forward intra-VLAN traffic (bridging) while also forwarding traffic between VLANs (routing), so

Egress Switch

This document is a guide to implementing and maintaining an Egress Switch secure data exchange infrastructure, covering best practice security, recommendatory and mandatory policies.

Configure egress gateways, on-premises | Calico

Configure specific application traffic to exit the cluster through an egress gateway. When traffic from particular applications leaves the cluster to access an external

Achieving Line-Rate Forwarding: Buffer Allocation and QoS

Core Architecture & Switching Logic: The Hardware Foundation for Line-Rate Forwarding The Huawei AR series is engineered to achieve high-throughput and low-latency performance through a purpose

Traefik Proxy v3.7: 85+ Ingress NGINX Annotations and More

Traefik Proxy 3.7 brings support for 85+ Ingress NGINX annotations, TLS certs in the dashboard, middlewares on services, full Gateway API v1.5 support, & more.

Deploying Firewalls as Egress Devices

Networking Requirements Two firewalls at the campus egress set up a hot standby group that functions as the egress gateway of the campus network to filter service traffic that enters and leaves the

Azure OpenAI Service Multitenant Load Balancing and Token Per

This example shows how a multitenant service can distribute requests evenly among multiple Azure OpenAI Service instances and manage tokens per minute (TPM)...

Resource exemption in Microsoft Defender for Cloud | Microsoft ...

Microsoft Defender for Cloud Blog Microsoft Defender for Cloud is a cloud-native application platform (CNAPP) that offers security and compliance from code to runtime, enhanced by

Connecting Firewalls to Egress Routers Directly

Connecting Firewalls to Egress Routers Directly Networking Requirements At the egress of a large campus network, core switches are directly connected to upstream firewalls and connected to egress

Egress Network Design

Egress Route Design Egress routes of the campus network are used for north-south communication between the campus intranet and external networks. When a firewall is used as the

Centralized egress to internet

For IPv6 traffic, egress traffic can be configured to leave each VPC through an egress only internet gateway in a decentralized manner or it can be configured to be sent to a centralized VPC using NAT

Egress Network Configuration

Egress Network Configuration In this case, the firewall is used as the security egress gateway. To implement secure communication between the campus network and external network,

Contact Us

Continue your research online:

Website: <https://alfa-pro.co.za>

Technical inquiry: <https://alfa-pro.co.za/contact.html>

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

