Basefarm: Scaling Intrusion Detection Systems with DANZ Monitoring Fabric (DMF)

Highlights

Challenge

- Implement cost-effective intrusion detection across multiple data centers
- Reduce time-to-deploy and minimize operational overhead

Solutions

- DANZ Monitoring Fabric - Out-of-Band
- Dell S4048-ON Switch Hardware

Results

- Existing tools span multiple data centers, eliminating the need for more than one IDS solution
- Ease of management and fast deployment, including integration and automation of workflows
- Ability to enable every tool, regardless of location, to receive real-time copies of relevant network flows

Basefarm is a leading hosting provider for critical business applications, currently hosting more than 35,000 services that reach more than 40 million end-users globally through its data centers in Amsterdam, Netherlands, Oslo, Norway, and Stockholm, Sweden. Basefarm customers require unique, high-performance solutions that support their mission-critical applications at all times, and ever-evolving needs. Providing IT services for companies with high volumes of traffic, increasingly shorter time-to-market windows, and demand for stringent security is no simple feat. That is why Basefarm is in business: to support its customers' success with superior technological solutions.

The Need for a Scale-out Intrusion Detection Solution

Basefarm has a growing number of customers who require an intrusion detection system (IDS) that can monitor and analyze incoming traffic to identify and mitigate potential threats. To cost-effectively secure each of its data centers, Basefarm needed to scale its existing IDS solution from one data center to another. Basefarm also needed a way to optimize the IDS solution, so that it didn't get flooded with duplicate/unnecessary copied traffic.

Basefarm Investigates Solutions to Scale IDS Services

As a result, Basefarm began to investigate economical and easily scalable solutions that could meet its evolving needs. This is when Basefarm discovered DANZ Monitoring Fabric (DMF), a modern Network Packet Broker (NPB), that would allow Basefarm to extend its monitoring and security services across multiple data centers. DMF's SDN-based fabric architecture enables remote, centralized control of tool policies and configurations, with management performed through a simple, single pane of glass interface.

After a two-day proof of concept, Basefarm concluded that DMF is the ideal solution to enable it to cost-effectively scale intrusion detection services. For Basefarm, a key advantage of DMF is that it enables every tool, regardless of location, to receive real-time copies of relevant network flows. This superior design allows the entire visibility and security architecture to be operated and programmed through a single pane of glass.

Basefarm achieves Scale-out, Cost-effective Intrusion Detection for Multiple Data Centers

First-generation 'tap-to-tool' designs were simple: add more taps and span ports, and continue to give each organization its own dedicated taps for its dedicated tools. As each team added more tools, second-generation designs emerged: NPBs. This second design is the most common case today and leads to a "team-and-tool silo" condition. DMF is a third-generation design, that allows the networking team to break down these team-and-tool silos, converging on a multi-tenant monitoring fabric that can connect any tap to any tool at any time.

Today, Basefarm's intrusion detection system can monitor and analyze incoming network traffic to find and mitigate potential threats. This service is in many ways the "outermost" watch-post in regards to network security. The IDS offered through Basefarm has a self-learning approach, as everything that is discovered is added to the knowledge databases and uploaded to the network sensors for future use, which helps to prevent threats that could harm a customer in the future. With its next-gen IDS, Basefarm can maximize security and stop dangerous traffic from penetrating the environment.

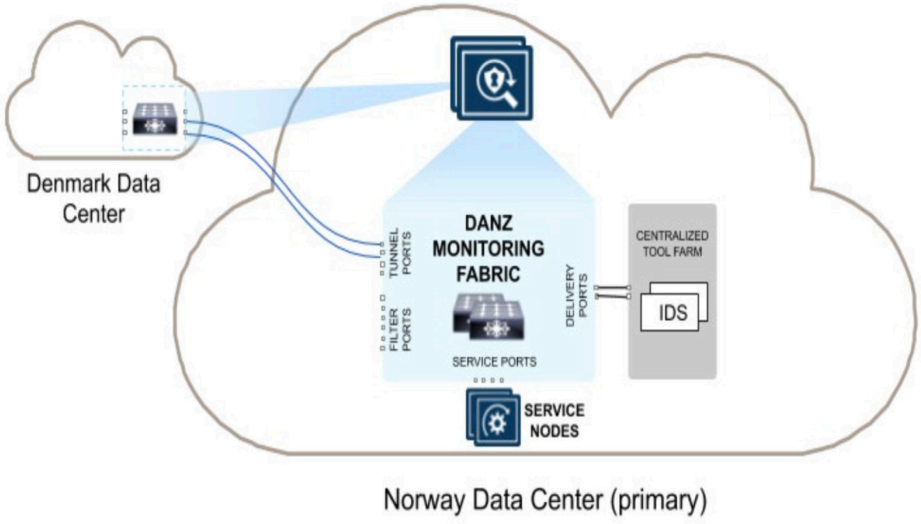
With DMF's support for overlapping policies and multi-tenant use cases, the operational workflows around a shared NPB infrastructure are practical in a way that was once out of reach. Basefarm is now able to deliver a secure, optimized platform for its customers without making additional tool investments. With DMF, Basefarm can connect two data centers by creating a tunnel between them, managed completely via the DMF controller. With DMF deployed as a multi-tenant NPB fabric, Basefarm quickly noticed positive changes in its operations, including improvements in its quality of service.

They also benefited considerably from DMF's:

- Flow Selection: Basefarm can now ensure that the right traffic is delivered to the appropriate tool by allowing for granular control of traffic delivery to each tool, aggregation, L2-L4 filtering, deeper packet matching, and sFlow generation.
- Ease of Management: A visually rich, drag-and-drop user interface offers valuable analytics in real-time. Integration of performance and security tools are enabled with Rest APIs, simplifying workflows.
- Advanced Packet Handling: Basefarm can now optimize the performance of its IDS solution through deduplication, packet slicing/masking, header stripping, and regular expression matching of customer traffic based on required flows.

In deploying DMF, Basefarm now has an easy, scalable, and economical solution to support its IDS.

The automation and ease of management provided by DMF enable Basefarm to provide mission-critical services to its customers, with room to grow.



Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062