FORTINET | USA

XPERTS

SUMMIT 2024

Helping you create a digitally secure future.

K8S 202 WORKSHOP - **FORTIWEB**

Srija Allam – Cloud Security Architect
Andy Wang – Consulting Systems Engineer
Robert Reris - Consulting Systems Engineer

XPERTS SUMMIT 2024

Goals

K8s 202 Workshop

- Learn K8s Security Concepts
- Build an AKS Cluster
- Install FortiWeb ingress controller
- WAF policy with TLS based ingress
- Perform SQL injection, URL rewriting
- Troubleshooting

Disclaimer

Fortinet Confidential

This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.

Agenda

1. Getting K8s Ready

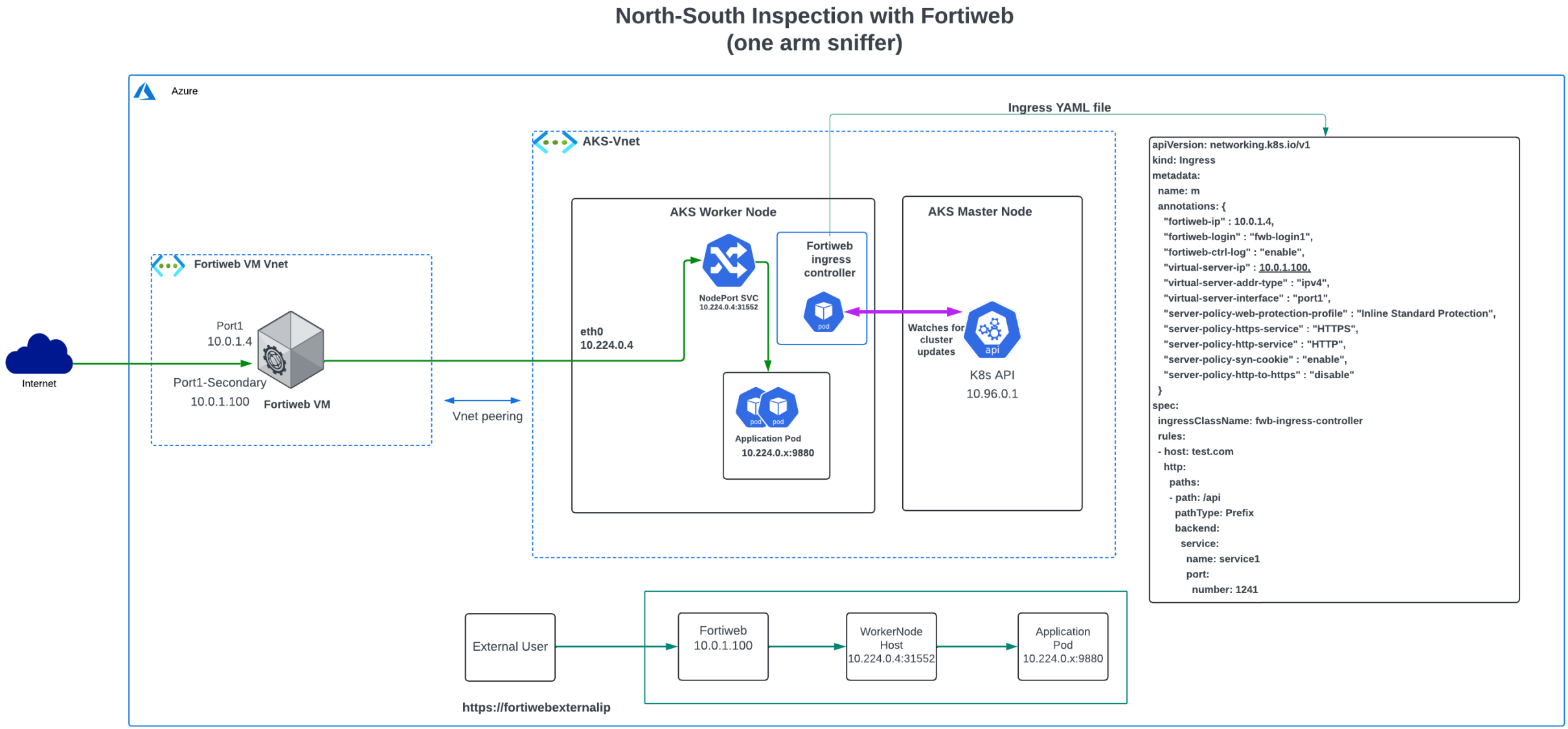
2. Intro to FortiWeb

3. Lab Time

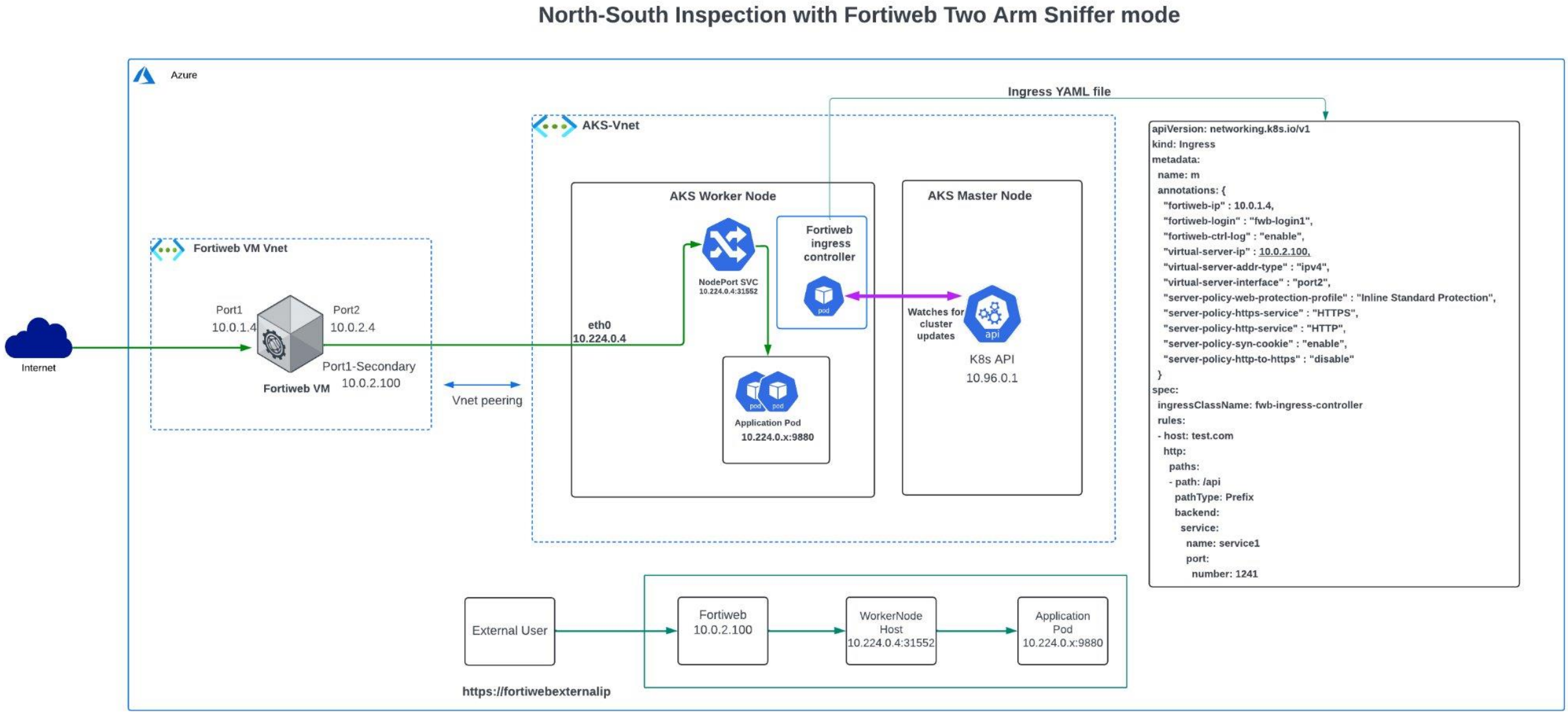
XPERTS SUMMIT 2024

Lab Architecture

One Arm Sniffer mode N-S inspection



Two Arm Sniffer mode N-S inspection



XPERTS SUMMIT 2024

Ingress Controller

Why is Ingress Controller Needed?

1. **Centralized Traffic Management**: It centralizes the traffic management, allowing for easy routing rules setup.
2. **Load Balancing**: Distributes incoming traffic across multiple pods, ensuring high availability and reliability.
3. **SSL Termination**: Manages SSL/TLS termination, providing secure connections to the services.
4. **Path-Based Routing**: Allows for routing traffic to different services based on the request path.
5. **Name-Based Virtual Hosting**: Supports routing based on the hostname, enabling multiple applications to run on the same IP address.

XPERTS SUMMIT 2024

Ingress Types

K8s Ingress Types

1. **Minimal Ingress:** A basic Ingress configuration that routes traffic to a single backend service

2. **Simple fanout:** This Ingress configuration routes traffic to multiple services based on the URL path.

3. **Ingress with Default backend:** This Ingress configuration includes a default backend service that handles any requests that do not match any defined rules.

4. **TLS Ingress:** An Ingress configuration that secures traffic using TLS (HTTPS). It involves using certificates to encrypt traffic between clients and services, ensuring secure communication.

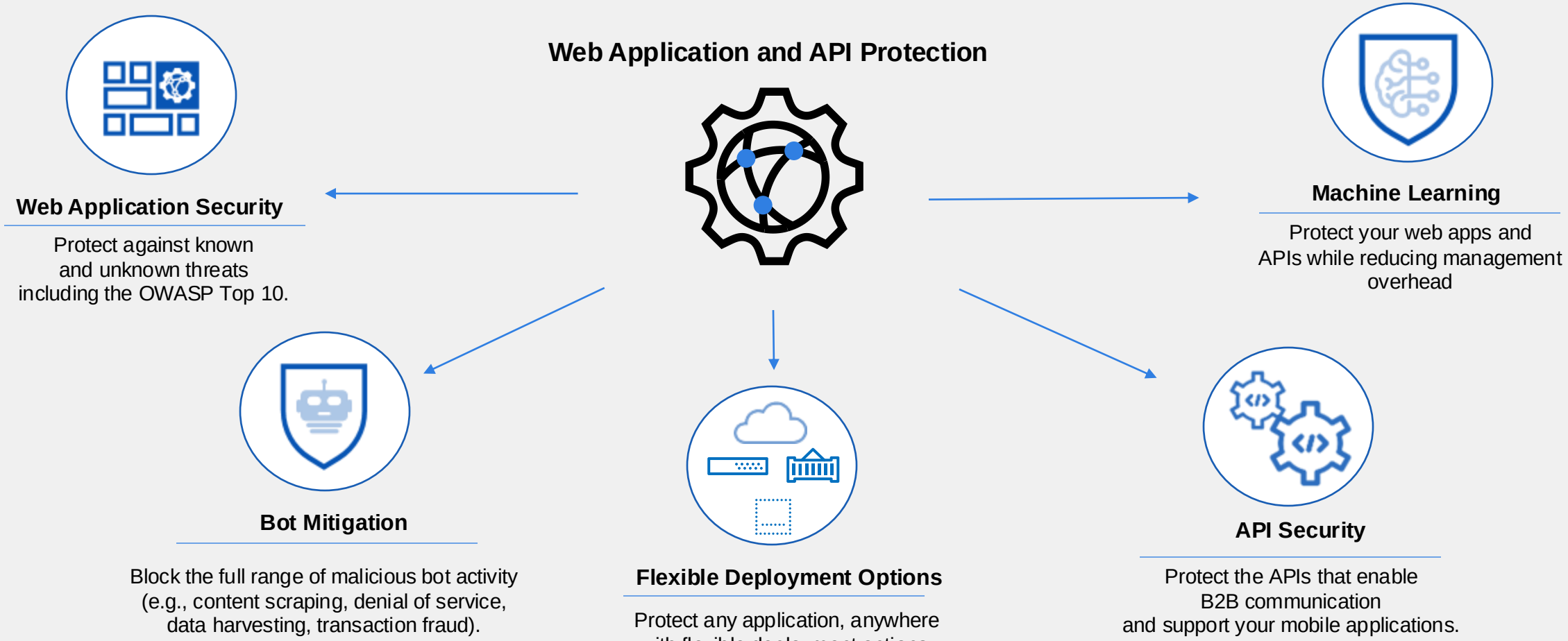
5. **Wildcard Ingress:** This Ingress allows for routing traffic based on wildcard domain names (e.g., *.example.com)

6. **Default backend:** The default backend is a service that handles requests that do not match any Ingress rules.

XPERTS SUMMIT 2024

FortiWeb

FortiWeb Web Application Firewall offers



SQL injection

SQL injection is a code injection technique that allows an attacker to interfere with the queries that an application makes to its database. It typically occurs when an application does not properly sanitize user inputs before including them in SQL queries. This vulnerability can allow attackers to:

- Bypass authentication.
- Access, modify, or delete data.
- Execute administrative operations on the database.

Example:

SELECT * FROM users WHERE username = 'input_username' AND password = 'input_password';

URL rewriting

URL rewriting is the process of modifying the URL of a web page dynamically. This can be done to make URLs more user-friendly or to mask the underlying implementation details. For example:

- **Original URL:** https://example.com/index.php?page=contact
- **Rewritten URL:** https://example.com/contact

URL rewriting is typically implemented through server configurations (e.g., .htaccess in Apache) or within the application code itself.

Troubleshooting

1. Diagnosing Network Connectivity Issues

2. For Kubernetes ingress controller

Example:

Kubectl logs *first-release-fwb-k8s-ctrl-59db65cddc-g4298* –n *fortiwebingress*