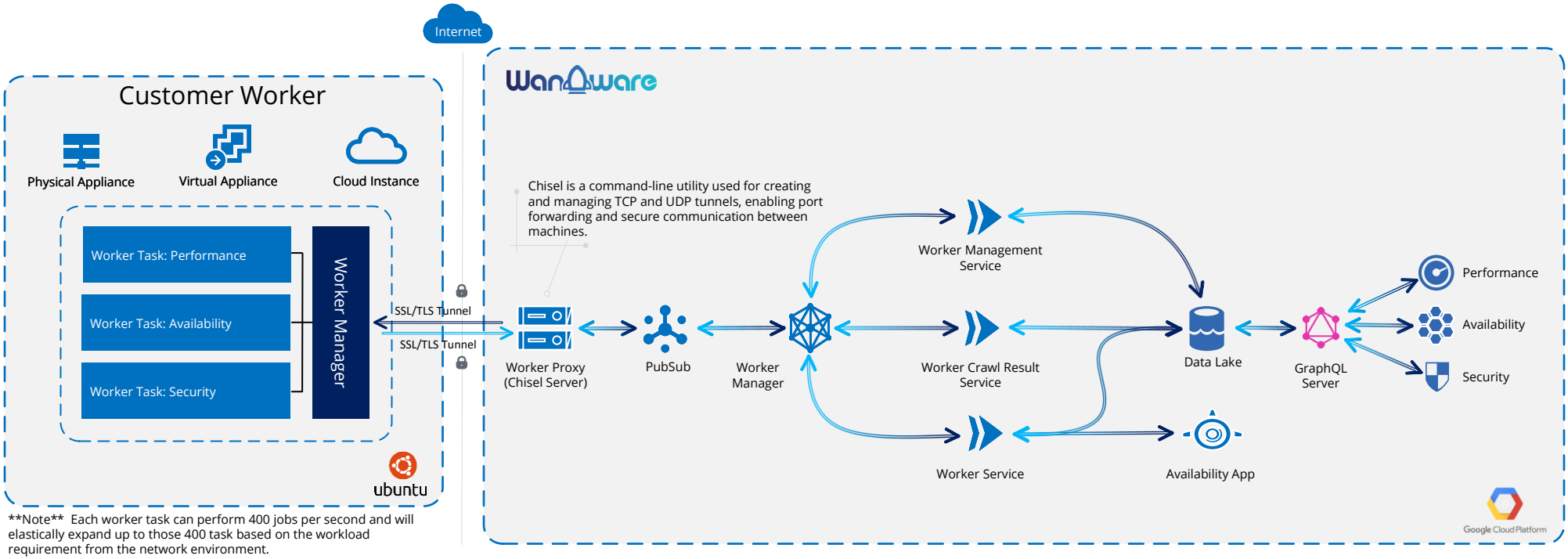
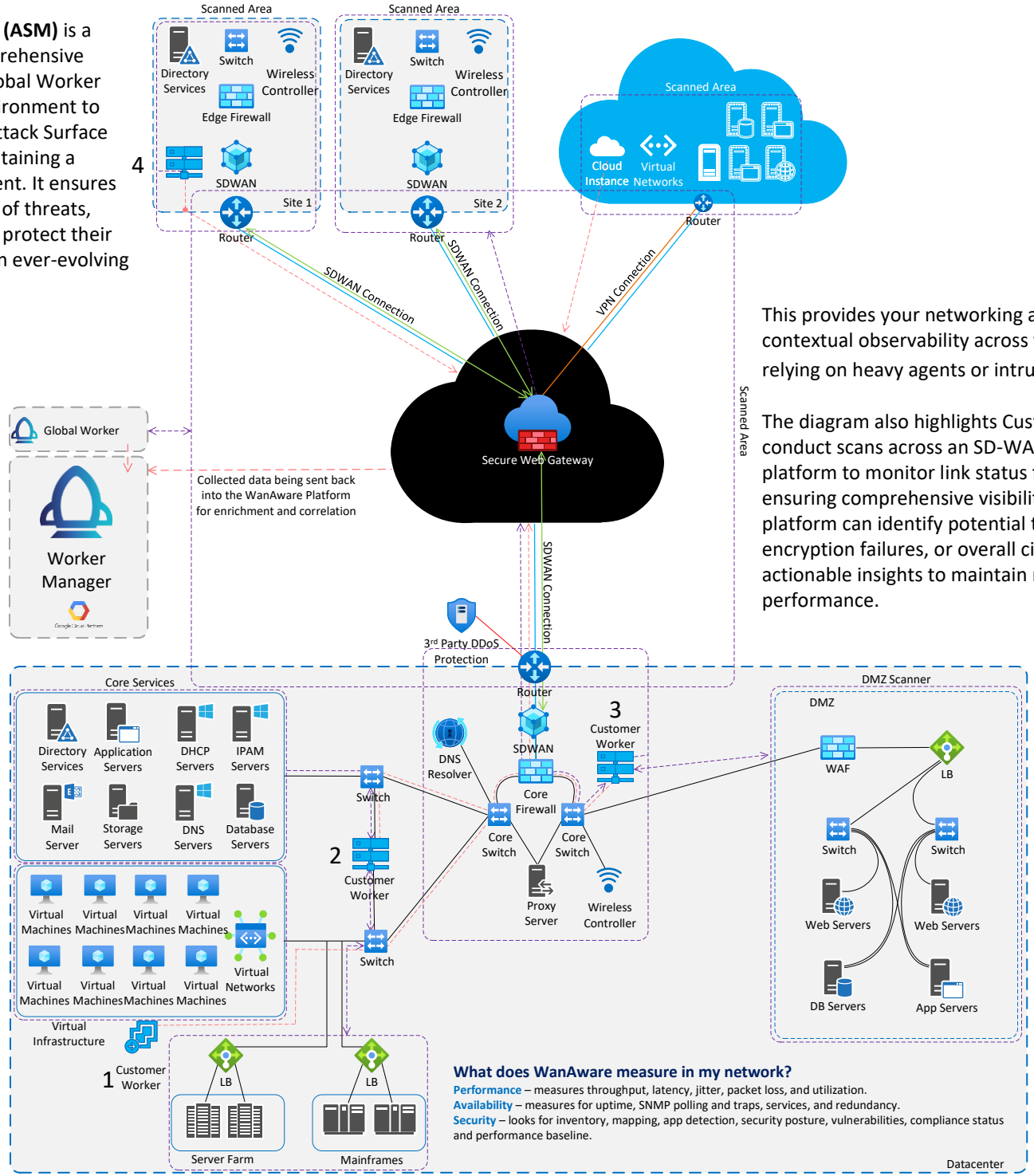
WanAware Customer Worker Architecture



Note Each worker task can perform 400 jobs per second and will elastically expand up to those 400 task based on the workload requirement from the network environment.

WanAware Customer Scan Architecture

Attack Surface Management (ASM) is a critical component of a comprehensive cybersecurity strategyThe Global Worker scans the external of the environment to identify the attack surface. Attack Surface Management is vital for maintaining a secure, resilient IT environment. It ensures organizations can stay ahead of threats, comply with regulations, and protect their reputation and assets from an ever-evolving threat landscape.



This section of the diagram illustrates how a diverse network deployment can be monitored comprehensively. By strategically deploying WanAware Customer Workers across the enterprise—whether as physical or virtual instances—organizations gain the flexibility and scalability to cover their entire environment effectively.

With its straightforward deployment process and robust capabilities, the Customer Worker can:

- Perform up to 400 tasks per task type per second
- Collect responses from monitored assets
- Relay this data back to the WanAware platform.

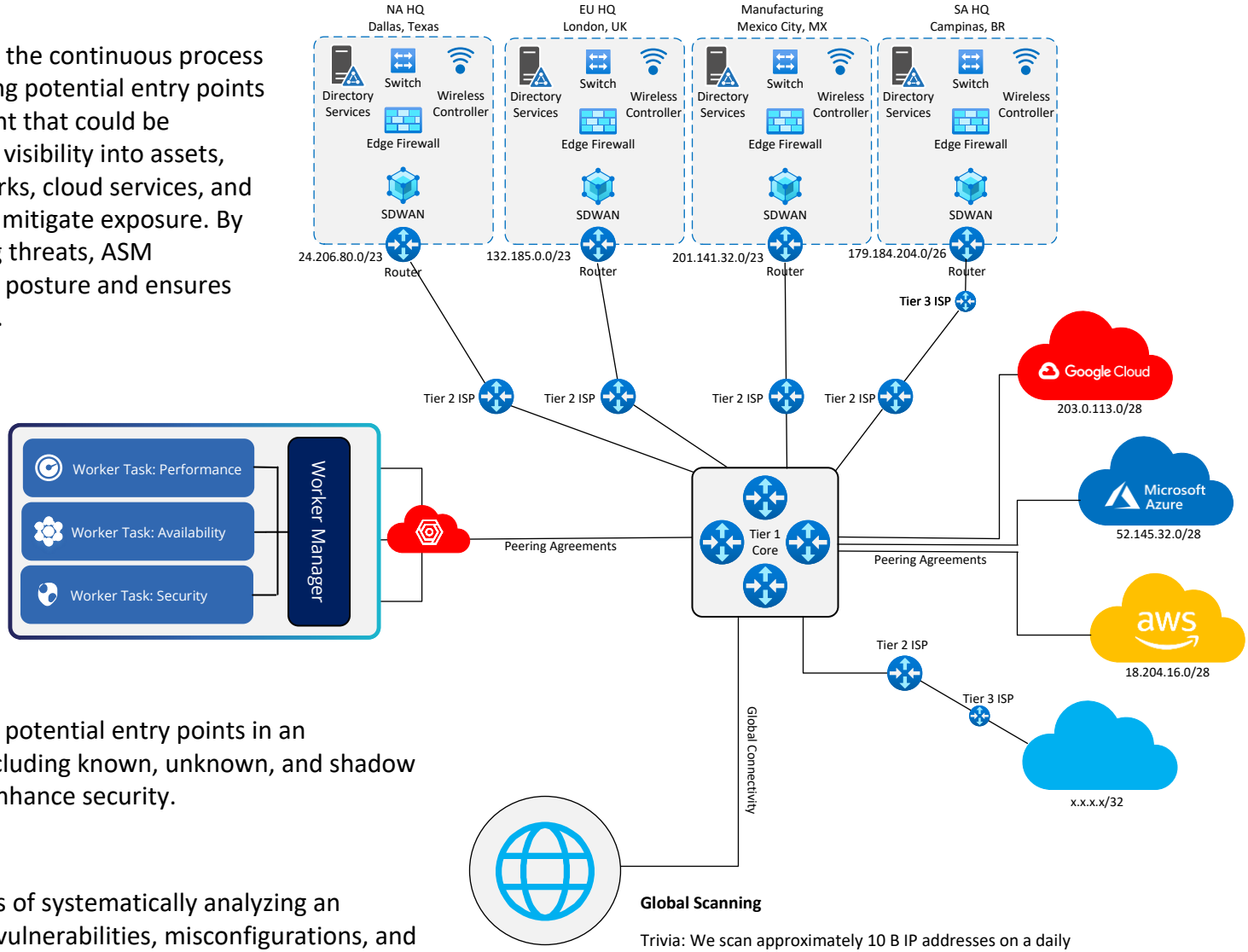
This provides your networking and security teams with detailed, contextual observability across the infrastructure—all without relying on heavy agents or intrusive service credentials.

The diagram also highlights Customer Worker 3, configured to conduct scans across an SD-WAN link. This setup allows the platform to monitor link status from inception to termination, ensuring comprehensive visibility. By scanning across links, the platform can identify potential threats such as tunnel leakage, encryption failures, or overall circuit degradation, providing actionable insights to maintain network integrity and performance.

WanAware Global Scan Architecture

An external scan begins by specifying the target subnet for scanning, followed by a traceroute to define the path and route to the attack surface. This initial mapping identifies the route to the destination, enabling the scanner to perform deeper scans on the subnet to assess the attack surface's condition. The discovery results provide baseline information essential for developing a comprehensive Attack Surface Management (ASM) plan.

Attack Surface Management (ASM) is the continuous process of identifying, monitoring, and reducing potential entry points in an organization's digital environment that could be exploited by cyber threats. It provides visibility into assets, vulnerabilities, and risks across networks, cloud services, and third-party integrations to proactively mitigate exposure. By continuously assessing and prioritizing threats, ASM strengthens an organization's security posture and ensures compliance with regulatory standards.



Attack Surface Discovery identifies all potential entry points in an organization's digital environment, including known, unknown, and shadow assets, to reduce vulnerabilities and enhance security.

Attack Surface Scanning is the process of systematically analyzing an organization's digital assets to detect vulnerabilities, misconfigurations, and exposures that could be exploited by attackers.

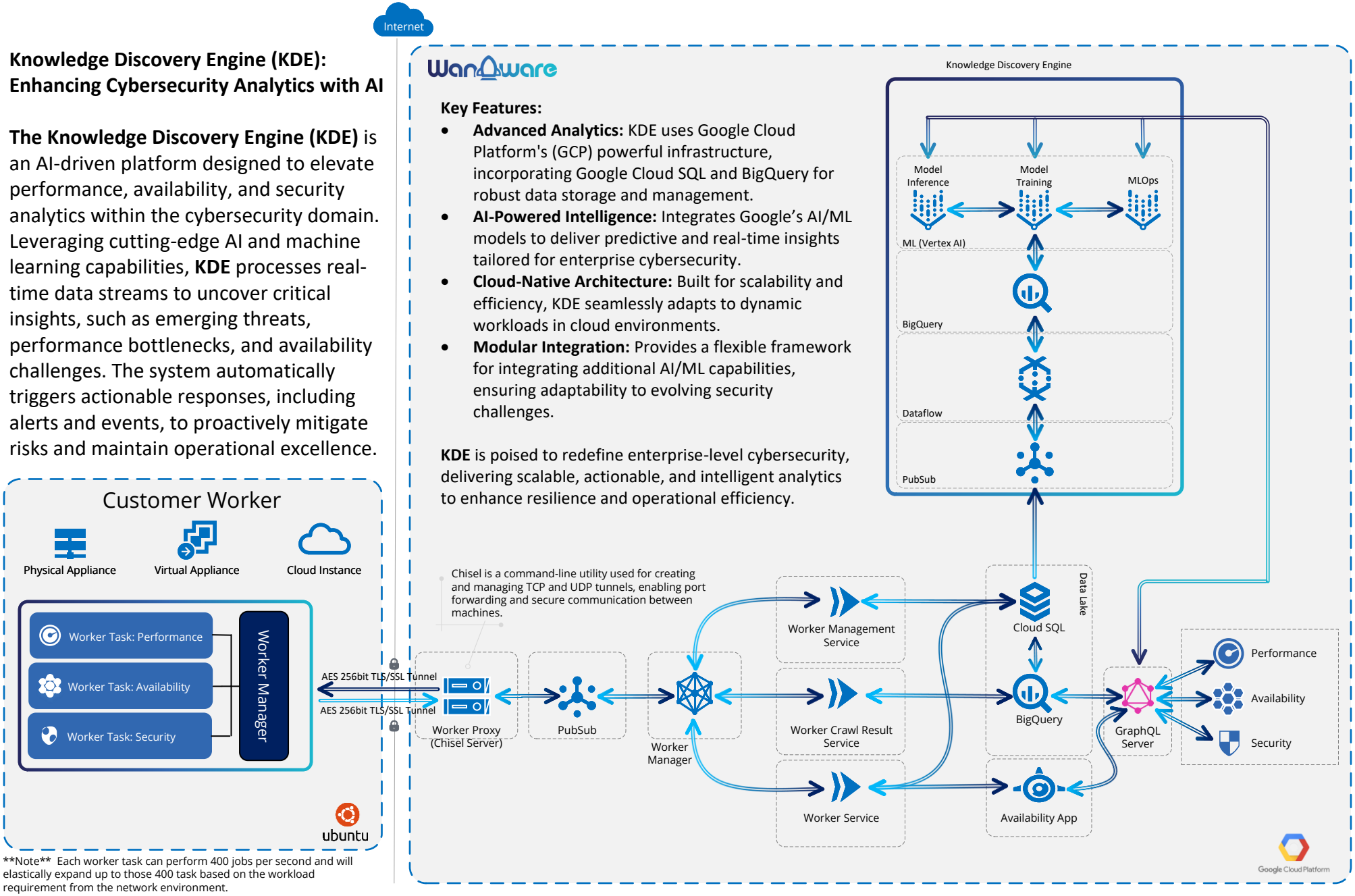
Global Scanning

Trivia: We scan approximately 10 B IP addresses on a daily basis. How many /1 subnets does that equate to?
The answer is below our logo.

WanAware Knowledge Discovery Engine Architecture

Knowledge Discovery Engine (KDE): Enhancing Cybersecurity Analytics with AI

The Knowledge Discovery Engine (KDE) is an AI-driven platform designed to elevate performance, availability, and security analytics within the cybersecurity domain. Leveraging cutting-edge AI and machine learning capabilities, **KDE** processes real-time data streams to uncover critical insights, such as emerging threats, performance bottlenecks, and availability challenges. The system automatically triggers actionable responses, including alerts and events, to proactively mitigate risks and maintain operational excellence.



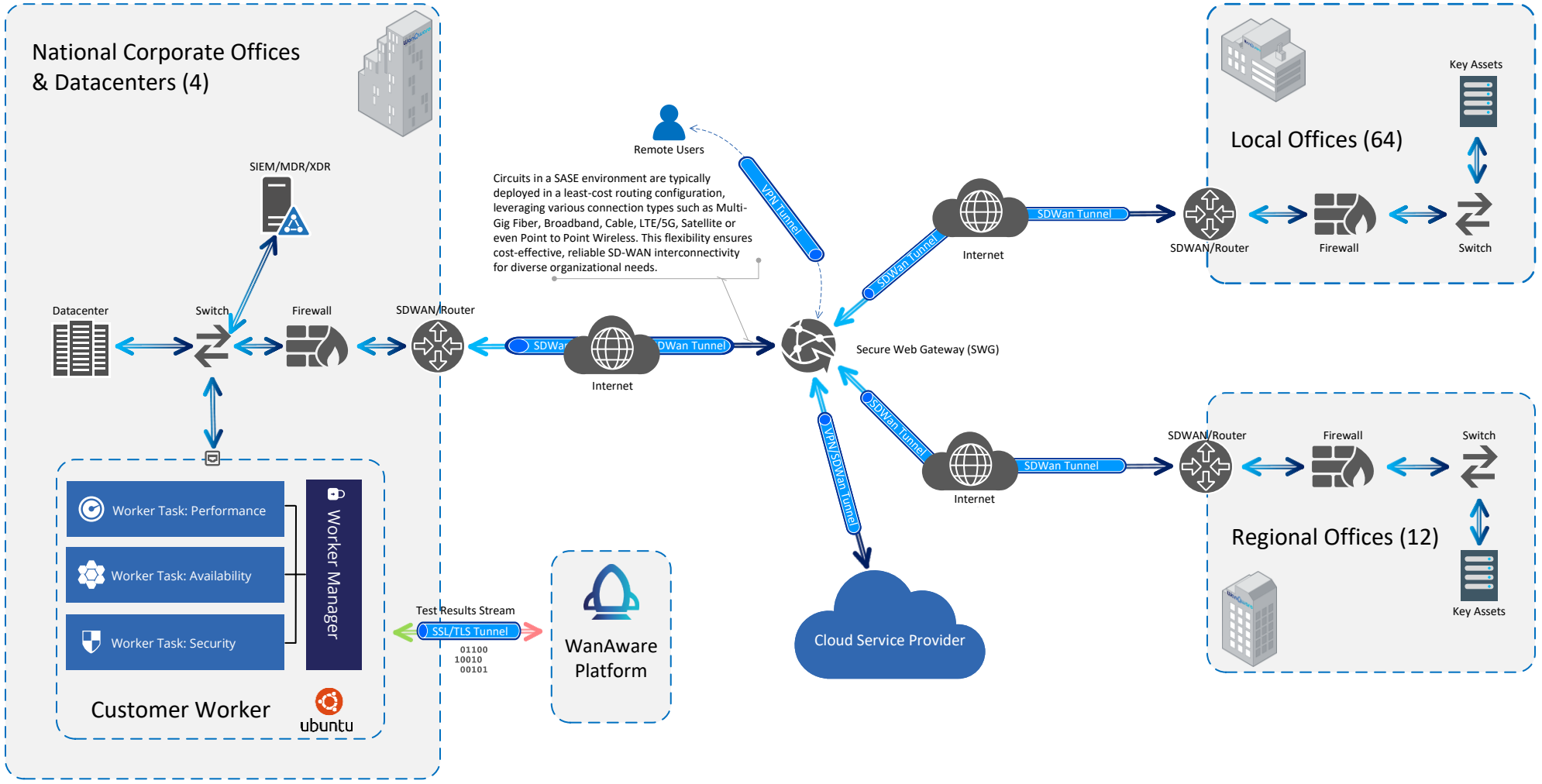
Key Features:

- **Advanced Analytics:** KDE uses Google Cloud Platform's (GCP) powerful infrastructure, incorporating Google Cloud SQL and BigQuery for robust data storage and management.
- **AI-Powered Intelligence:** Integrates Google's AI/ML models to deliver predictive and real-time insights tailored for enterprise cybersecurity.
- **Cloud-Native Architecture:** Built for scalability and efficiency, KDE seamlessly adapts to dynamic workloads in cloud environments.
- **Modular Integration:** Provides a flexible framework for integrating additional AI/ML capabilities, ensuring adaptability to evolving security challenges.

KDE is poised to redefine enterprise-level cybersecurity, delivering scalable, actionable, and intelligent analytics to enhance resilience and operational efficiency.

Note Each worker task can perform 400 jobs per second and will elastically expand up to those 400 task based on the workload requirement from the network environment.

WanAware in a SASE Environment (Distributed Enterprise)



WanAware Availability, Performance and Security (APS) Best Practices for SASE

When monitoring a distributed WAN using **SASE**, best practices include:

1. Focusing on network traffic and bandwidth utilization
2. Closely monitoring latency and packet loss
3. Actively tracking security events and firewall activity
4. Assessing application performance
5. Monitoring user and device access
6. Utilizing the SASE vendor's built-in monitoring capabilities to:
    - Gain comprehensive visibility across your distributed network
    - Ensure you monitor key aspects like:
        - VPN connections
        - Cloud Service Connectivity
        - Zero Trust Network Access (ZTNA) metrics In order to maintain optimal performance and security.

Key areas to monitor with SASE:

Network Performance:

- Bandwidth utilization across network segments
- Latency and packet loss on critical connections
- Throughput on different network links

Security Monitoring:

- Firewall logs and alerts
- Intrusion detection and prevention system (IDS/IPS) activity
- Malware detection and prevention
- User access controls and suspicious login attempts

Application Performance:

- Application response times
- Application latency and packet loss
- User experience metrics

Cloud Connectivity:

- Cloud service performance
- Latency to cloud-based applications
- Cloud service access controls

Zero Trust Network Access (ZTNA):

- ZTNA session monitoring
- Access control policies effectiveness

VPN Monitoring:

- VPN connection health
- VPN tunnel performance

Best practices for effective SASE monitoring:

Choose a SASE vendor with robust monitoring capabilities:

- Select a provider with a comprehensive monitoring platform that integrates seamlessly with your existing network infrastructure.

Set clear performance baselines:

- Establish expected network performance metrics to identify anomalies and potential issues quickly.

Leverage centralized dashboards:

- Utilize a single dashboard to visualize network health across your distributed environment for easier analysis.

Implement real-time alerts:

- Configure alerts for critical events like high latency, excessive packet loss, or security breaches to enable prompt response.

Utilize automated root cause analysis:

- Employ tools that can identify the source of network issues automatically to expedite troubleshooting.

Regularly review monitoring configurations:

- assess your monitoring sPeriodically ettings to ensure they remain relevant and effective as your network evolves.

Integrate with existing security tools:

Connect your SASE monitoring with existing seCurity solutions to provide a holistic view of network threats.

Best practices for effective SASE monitoring:

Choose a SASE vendor with robust monitoring capabilities:

- Select a provider with a comprehensive monitoring platform that integrates seamlessly with your existing network infrastructure.

Set clear performance baselines:

- Establish expected network performance metrics to identify anomalies and potential issues quickly.

Leverage centralized dashboards:

- Utilize a single dashboard to visualize network health across your distributed environment for easier analysis.

Implement real-time alerts:

- Configure alerts for critical events like high latency, excessive packet loss, or security breaches to enable prompt response.

Utilize automated root cause analysis:

- Employ tools that can identify the source of network issues automatically to expedite troubleshooting.

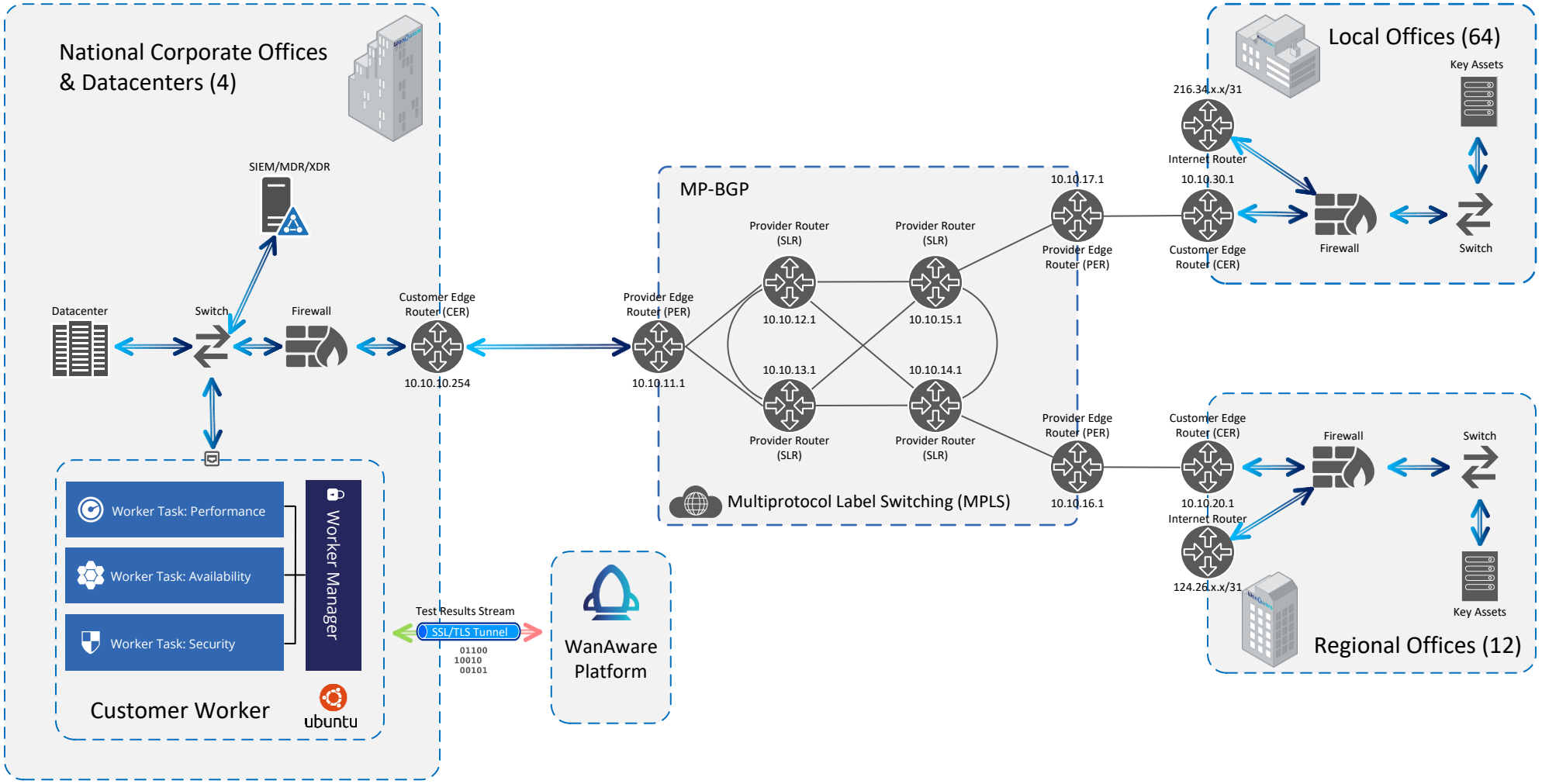
Regularly review monitoring configurations:

- assess your monitoring sPeriodically ettings to ensure they remain relevant and effective as your network evolves.

Integrate with existing security tools:

- Connect your SASE monitoring with existing seCurity solutions to provide a holistic view of network threats.

WanAware in a MPLS Environment (Distributed Enterprise)



Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a high-performance routing technique used in telecommunications networks to direct data from one node to another based on short path labels rather than long network addresses. This method streamlines the data flow, improves speed, and enhances overall efficiency in the network.

WanAware in a MPLS Environment (Distributed Enterprise)

Testing and monitoring an MPLS network are essential to ensure its performance, reliability, and adherence to service level agreements (SLAs). Here are the best practices for MPLS testing and monitoring:

1. Establish Performance Benchmarks

- **Define SLAs:** Set clear metrics for latency, packet loss, jitter, and bandwidth utilization based on business requirements.
- **Baseline Measurements:** Conduct initial tests to establish a performance baseline under normal operating conditions.

2. Implement Comprehensive Monitoring

Use Specialized Tools:

- Tools like NetFlow, IPFIX, or MPLS-aware monitoring platforms provide visibility into traffic flows and bottlenecks.
- SNMP-based tools for device health and link status monitoring.

Monitor Key Metrics:

- **Latency:** Ensure low delays for time-sensitive applications like VoIP.
- **Jitter:** Maintain consistency for real-time services.
- **Packet Loss:** Monitor for signs of network congestion or errors.
- **Bandwidth Utilization:** Detect over-utilization or under-utilization of links.

3. Test Network Resiliency

- **Path Validation:** Use MPLS traceroute to confirm that Label Switched Paths (LSPs) are correctly established.
- **Failover Testing:** Simulate link or node failures to ensure the MPLS Fast Reroute (FRR) mechanism works as expected.
- **Traffic Engineering:** Test the efficiency of MPLS TE tunnels and their ability to redistribute traffic during peak loads.

4. Conduct Periodic Performance Testing

- **Active Testing:** Inject synthetic traffic to measure real-time performance metrics without relying on production data.
- **Passive Testing:** Analyze live traffic to assess actual network performance and detect anomalies.
- **QoS Verification:** Test priority queues to confirm that high-priority traffic (e.g., voice) gets preferential treatment.

5. Analyze Routing and Label Management

- **Routing Protocol Testing:** Test the interaction between MPLS and routing protocols (e.g., OSPF, IS-IS, or BGP).
- **Label Validation:** Verify that labels are correctly assigned and swapped throughout the MPLS network.

6. Monitor Network Health Continuously

- **Link-Level Monitoring:** Continuously monitor MPLS link statuses for errors (e.g., CRC errors) and performance degradation.
- **Path-Level Monitoring:** Monitor LSPs to ensure traffic follows the intended path without deviations.
- **Device Monitoring:** Track MPLS routers' CPU and memory usage to avoid overloading.

7. Leverage SLA Monitoring Tools

- **Service Assurance Tools:** Use tools like Cisco IPSLA or Juniper RPM to monitor SLA compliance in real time.
- **Threshold Alerts:** Set alerts for SLA violations like excessive latency or packet loss.

8. Automate Testing and Monitoring

- **Automation Frameworks:** Deploy solutions that automate performance tests and trigger remediation workflows.
- **AI/ML for Anomaly Detection:** Use machine learning-based monitoring tools to detect and predict unusual traffic patterns.

9. Test Security Measures

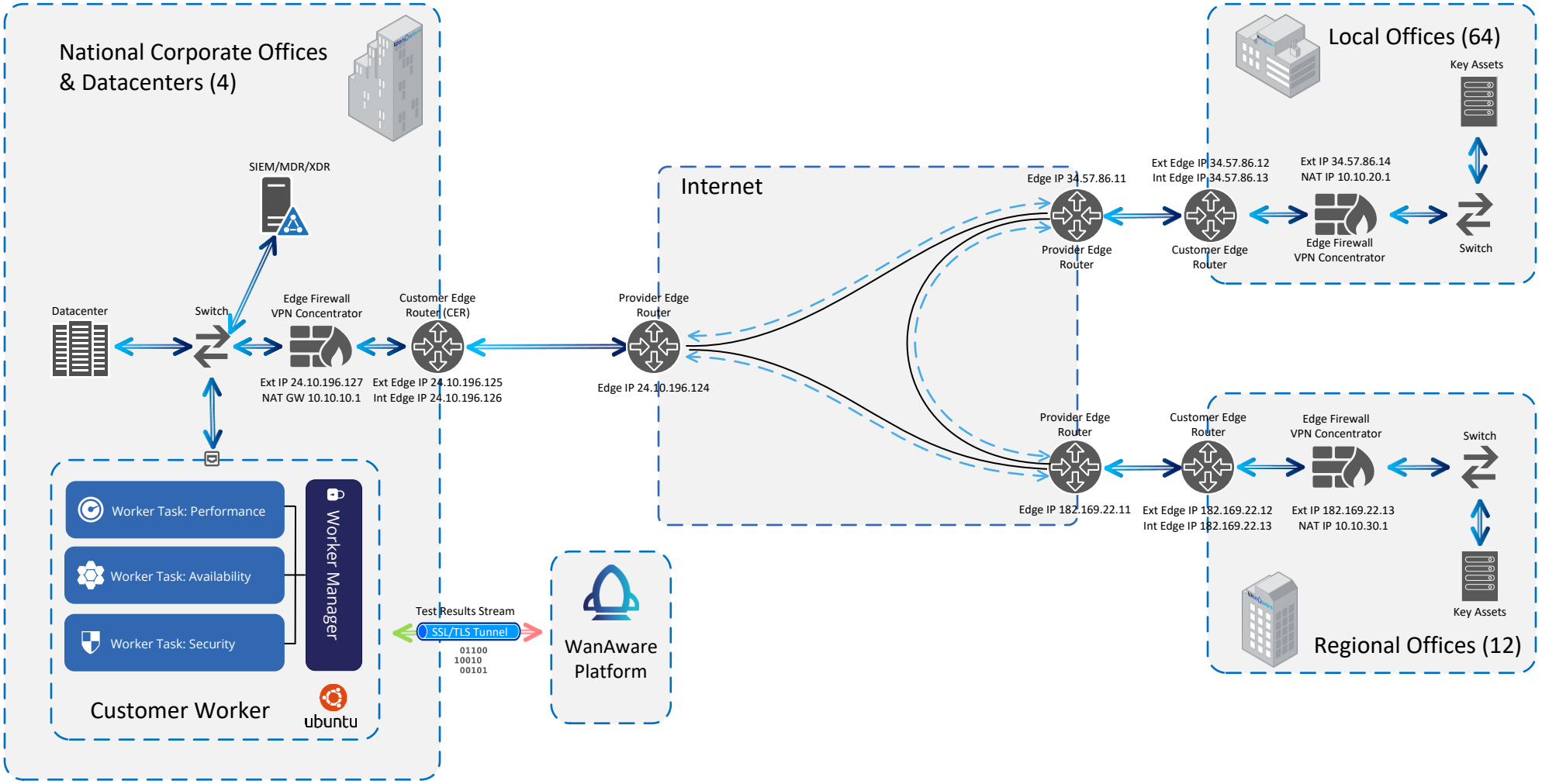
- **Traffic Segmentation:** Verify the isolation of MPLS VPN traffic to prevent cross-contamination.
- **DoS/DDoS Resilience:** Simulate attacks to ensure the MPLS network can handle traffic spikes and maintain performance.

10. Reporting and Analytics

- **Real-Time Dashboards:** Provide visual insights into network health and performance.
- **Historical Analysis:** Store and analyze historical data to identify trends and predict future issues.
- **SLA Compliance Reports:** Generate detailed reports for internal and external stakeholders to ensure SLA adherence.

Regular MPLS testing and monitoring ensures that the network delivers consistent and reliable performance while meeting business and operational needs.

WanAware in a VPN Environment (Distributed Enterprise)



Virtual Private Networking (VPN)

An enterprise VPN network provides secure, encrypted remote access for employees, partners, or devices to connect to a corporate network over the internet. It ensures data confidentiality and integrity through tunneling protocols like IPSec or SSL/TLS while enforcing authentication mechanisms such as MFA. Scalable and centrally managed, it supports hybrid work environments, enabling seamless access to resources across various locations while maintaining strict security controls.

WanAware in a VPN Based Environment (Distributed Enterprise)

Testing and monitoring an enterprise VPN network are crucial for ensuring secure, efficient, and reliable remote connectivity. Here are some best practices:

1. Testing the VPN Network

Performance Testing

- **Bandwidth and Latency:** Measure upload/download speeds and latency to identify potential bottlenecks.
- **Stress Testing:** Simulate heavy traffic loads to assess the VPN's ability to handle concurrent users.
- **Packet Loss and Jitter:** Test for packet integrity and transmission consistency, critical for VoIP and real-time applications.
- **Failover Testing:** Simulate link failures to ensure seamless failover in high-availability configurations.

Security Testing

- **Penetration Testing:** Identify vulnerabilities in encryption protocols, authentication mechanisms, and VPN gateways.
- **Configuration Audit:** Ensure secure protocols (e.g., IPSec, SSL/TLS) are correctly configured and not using deprecated methods like PPTP.
- **Access Control Verification:** Validate that access control policies enforce least privilege.
- **Vulnerability Scans:** Regularly scan VPN servers and client devices for known vulnerabilities.

User Testing

- **Authentication Flow:** Test MFA or SSO mechanisms for usability and security.
- **Device Compatibility:** Verify the VPN client's compatibility across all supported operating systems and devices.
- **Connection Stability:** Simulate real-world usage scenarios to test stability over time and different networks (e.g., Wi-Fi, cellular).

2. Monitoring the VPN Network

Performance Metrics

- **Connection Metrics:** Monitor concurrent connections, session duration, and connection success rates.
- **Traffic Metrics:** Track data usage, throughput, and traffic types to identify abnormal patterns.
- **Latency and Uptime:** Continuously monitor latency and ensure SLA adherence for uptime.

Security Metrics

- **Anomalous Login Attempts:** Identify repeated failed logins or logins from unusual geolocations.
- **Data Leakage:** Monitor for unauthorized data transfer through VPN tunnels.
- **Encryption Integrity:** Ensure VPN sessions are encrypted and not downgraded due to misconfigurations.

System Metrics

- **CPU and Memory Utilization:** Ensure VPN servers and appliances have sufficient resources.
- **Disk Space:** Monitor log file storage to prevent overflow and loss of data.
- **Firmware/Software Updates:** Keep track of outdated software or firmware that may pose security risks.

3. Tools for Testing and Monitoring

- **Performance Monitoring Tools:** Tools like SolarWinds, PRTG, and Nagios for real-time performance monitoring.
- **SIEM Solutions:** Integrate VPN logs into SIEM platforms like Splunk or QRadar to correlate events and detect threats.
- **Endpoint Detection Tools:** Use solutions like CrowdStrike or SentinelOne for monitoring endpoint VPN client activity.
- **Network Monitoring Tools:** Leverage NetFlow or sFlow analysis for traffic and flow monitoring.
- **Synthetic Testing Tools:** Use tools like iPerf or Wireshark for packet-level testing and performance diagnostics.

4. Automation and Alerting

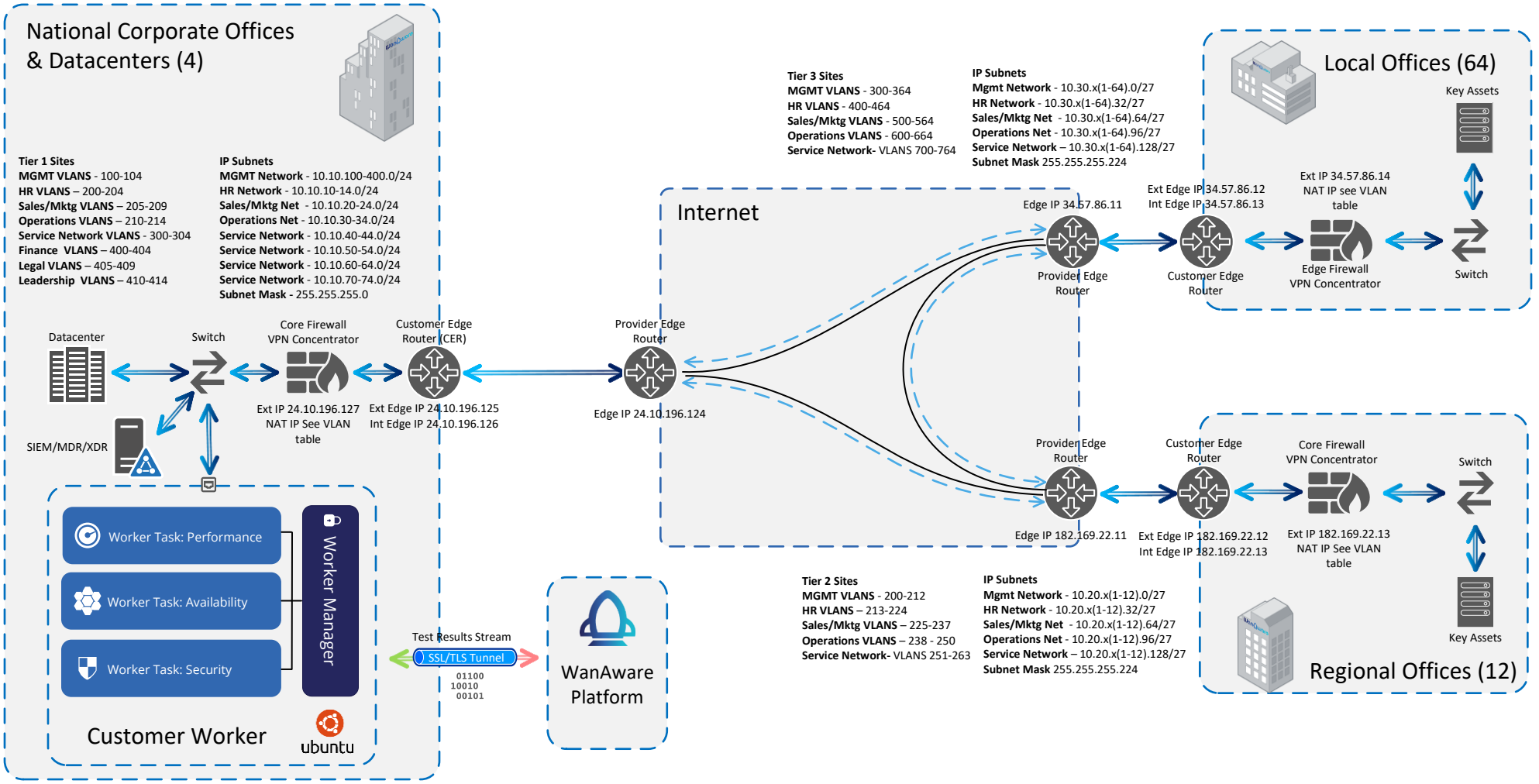
- **Automate Testing:** Schedule regular automated performance and security tests.
- **Threshold Alerts:** Configure alerts for thresholds like high latency, resource overuse, or abnormal connection patterns.
- **Proactive Issue Resolution:** Use AI-based monitoring tools to predict and resolve issues before they impact users.

5. Periodic Reviews

- **Policy Updates:** Regularly review VPN policies to adapt to changes in network or user requirements.
- **Audit Logs:** Periodically audit VPN logs for compliance and forensic purposes.
- **User Feedback:** Collect feedback from users to identify and address usability issues.

By implementing these best practices, organizations can ensure their enterprise VPN network is robust, secure, and capable of meeting both operational and security needs.

WanAware in a VLAN Segmented Environment (Distributed Enterprise)



Virtual Local Area Network (VLAN) (also known as Network Segmentation)

A Virtual Local Area Network (VLAN) is a logical grouping of devices within a physical network that are segmented to act as if they are on separate, isolated networks. VLANs are used in network segmentation to enhance security and performance by dividing a single physical network into multiple distinct broadcast domains, reducing unnecessary traffic between devices. By isolating specific devices or applications into separate VLANs, organizations can limit access, reduce the attack surface, and improve traffic management across the network.

WanAware in a VLAN Segmented Environment (Distributed Enterprise)

Testing and monitoring an enterprise network employing VLANs for network segmentation is crucial for ensuring performance, security, and compliance. Here's a step-by-step guide:

1. Testing a VLAN-Segmented Network

Performance Testing
- **Inter-VLAN Traffic:** Verify connectivity between VLANs using Layer 3 routing or gateways.
- Test routing protocols (e.g., OSPF, BGP) or Layer 3 switches for expected behavior.
- **Bandwidth Utilization:** Use tools like iPerf to measure throughput within and across VLANs.
- **Latency Testing:** Measure latency for communication between devices within the same VLAN and across VLANs.
- **Broadcast Containment:** Generate broadcast traffic to test that broadcasts are confined within a VLAN.

Configuration Validation
- **VLAN ID and Port Mapping:** Check VLAN assignments for access ports and trunk ports on switches.
- **Access Control Lists (ACLs):** Validate ACL rules for traffic filtering between VLANs.
- **Spanning Tree Protocol (STP):** Test STP to prevent loops in VLAN environments, ensuring optimal path selection.

Isolation Testing
- **Communication Restriction:** Ensure VLANs are isolated as per the design and policy (e.g., IoT devices cannot communicate with sensitive finance VLANs).
- **Unauthorized Traffic Detection:** Simulate traffic to test whether unintended VLANs can access restricted resources.

Security Testing
- **VLAN Hopping Attacks:** Test for vulnerabilities like double tagging or switch spoofing using penetration testing tools.
- **Authentication Mechanisms:** Verify 802.1X or other authentication protocols for VLAN access.

Redundancy and Failover Testing
- **Trunk Failover:** Simulate link failures on trunk ports to ensure VLAN traffic reroutes correctly.
- **Device Failures:** Test failover mechanisms on routers or Layer 3 switches handling inter-VLAN routing.

2. Monitoring a VLAN-Segmented Network

Performance Monitoring
- **Traffic Flow Analysis:** Use tools like NetFlow, sFlow, or IPFIX to monitor inter-VLAN traffic patterns and volume.
- **Bandwidth Utilization:** Monitor trunk ports and access ports to identify over-utilized links.
- **Latency and Jitter:** Continuously measure these metrics to detect potential network issues.

Security Monitoring
- **Intrusion Detection Systems (IDS):** Deploy IDS/IPS tools to monitor VLAN-segmented traffic for anomalies.
- **Unauthorized Access Attempts:** Log and analyze attempts to access restricted VLANs.
- **Traffic Anomalies:** Look for unusual spikes in traffic or unexpected inter-VLAN communication.

System Health Monitoring
- **Switch Health:** Monitor CPU, memory, and temperature on switches managing VLANs.
- **Spanning Tree Topology:** Track STP status to ensure the network topology remains stable.
- **VLAN Status:** Verify VLAN states (active/inactive) on all switches.

Log and Event Monitoring
- **Syslog Servers:** Collect and analyze logs from switches, routers, and firewalls for VLAN-related events.
- **SNMP Monitoring:** Use SNMP-based tools like SolarWinds or PRTG to track VLAN metrics in real-time.
- **SIEM Integration:** Feed logs into a Security Information and Event Management (SIEM) tool for correlation and advanced analysis.

3. Tools for Testing and Monitoring VLANs

- **Performance Tools:** iPerf, SolarWinds NPM, PRTG, Nagios
- **Packet Analyzers:** Wireshark, tcpdump
- **Traffic Analysis:** NetFlow Analyzer, sFlow Collector
- **Security Tools:** Kali Linux (for penetration testing), Nessus, or Nmap
- **Switch-Specific Tools:** Vendor-specific solutions like Cisco Prime Infrastructure or Aruba AirWave

4. Best Practices

- **Automated Monitoring:** Set up alerts for key metrics like high utilization, abnormal traffic patterns, or VLAN configuration changes.
- **Regular Audits:** Periodically audit VLAN configurations, ACLs, and routing protocols.
- **Backup Configurations:** Maintain backups of switch/router configurations for VLANs.
- **Segmentation Policies:** Ensure VLAN policies align with business and security requirements.
- **Baseline Performance:** Establish baseline metrics for VLAN traffic to quickly detect deviations.

By rigorously testing and continuously monitoring a VLAN-segmented enterprise network, organizations can ensure optimal performance, robust security, and alignment with operational objectives.