NetWolves

Intelligent Network Solutions

NETWOLVES CUSTOMER SERVICE AGREEMENT
MANAGED NETWORK OFFERING (MNO) TERMS

1. Scope

This document defines the Managed Network Services (“Services”) Customer is interested in purchasing. Only Services described in this MNO are included in NetWolves’ Managed Network Services, however, any service outside the scope of these Services may be available to Customer on a per occurrence basis at NetWolves’ then-current rates. Examples of services outside the scope of this MNO include, but are not limited to: a) service for equipment which is not in good operating condition, b) services related to installation, de-installation, movement of equipment or any related electrical requirements, c) service for Customer application software requirements including repairs due to virus damage, d) network and system administration requirements, and, e) service to isolate, identify and repair problems with network components not covered by this SOW, f) on-site support. Customer may contact NetWolves’ Engineering Support at any time concerning out of scope services.

2. Services

NetWolves will be responsible for remotely monitoring and/or managing Customer’s information technology infrastructure systems as identified in Schedule A, to be provided at the initial project launch meeting. NetWolves will manage and maintain all configurations and operation systems image files for all devices identified in the Schedule A

Real Time Remote Monitoring. NetWolves provides coverage seven (7) days a week, twenty-four (24) hours a day and three hundred sixty-five (365) days per year (7 x 24) for real time remote monitoring of Customer infrastructure.

Incident Management, as defined by NetWolves, is the processes and procedures created to identify, analyze and correct current and potential customer affecting issues to restore normal customer functionality and minimize customer down-time. These services include event detection and fault notification, fault isolation and diagnosis, remote resolution (where applicable), coordination/monitoring of resolution by third parties, escalation and reporting. These services are restricted to items identified in Schedule A, however, any/all levels of troubleshooting are available to any customer on a time and material basis. Incident tickets will be created to troubleshoot and track customer affecting outages or issues from inception to resolution.

NetWolves will provide 7 x 24 fault detection of Customer’s infrastructure-supported devices. NetWolves’ management tools react to the following possible fault scenarios: a) an alert notification is received from a managed device, or b) the management system does not receive a response from an active poll of the managed device on a regular basis.

Incident escalation will occur, if no solution is known or if no progress on a fault resolution is being made. NetWolves will monitor all incidents to ensure escalation and resolution times are being met and will contact Customer as required.

CPR (Critical Problem Review), as defined by NetWolves, is a service provided to MNS customers who would present the following:

- Detailed description of the outage
- Documented RFO (Reason for Outage)
- Timelines of the outage and what actions NetWolves SA teams took for resolution
- All personnel involved in the outage
- Remediation steps to prevent the RFO from reoccurring

The justification for NetWolves Service Assurance (“SA”) teams to produce a CPR is defined as a critical production outage affecting multiple customer sites for durations of 2 hours or more. This service can also be produced upon request by the customer at any time at time and materials cost.

RMAC (Reviews, Moves, Adds & Changes), as defined by NetWolves, is any requests that need to be completed which are estimated to require up to 8 hours to produce, design and implement by NetWolves SA/SD teams for an existing customer to currently operational managed devices.

ECP (Existing Client Project), as defined by NetWolves, is any changes that will need to be completed which are estimated to require more than 8 hours to design and implement by NetWolves Service Assurance (“SA”) / Service Delivery (“SD”) teams for an existing customer. ECP’s require a dedicated project manager, lead engineer and account manager participation as well as a signed SoW by the customer. All ECP estimates will tracked by the NetWolves account manager.

NetWolves reserves the right to revise the Services defined in Section 5 upon thirty (30) days’ notice to Customer.

3. Customer Responsibilities

Customer will be responsible for the following:

3.1. Customer will agree to and execute Schedule A which will include the overall service description of the services to be provided.

3.2. Customer agrees to provide NetWolves with access to Customer’s employees, contractors and other identified persons, as reasonably required by NetWolves, to support activities such as information gathering, information validation and interviews.

3.3. NetWolves cannot guarantee at the time of signing of this MNO, that all of Customer network devices can be monitored with SRM[2] or via Simple Network Management Protocol (SNMP) or that NetWolves has access through Customer’s network to all such devices. Customer will be responsible for certifying that all network devices can be monitored with either SRM^2 or SNMP, prior to NetWolves providing network monitoring and/or management services on such devices under this agreement, and that such devices will be accessible by NetWolves.

3.4. Certain Services may require the placement of unattended equipment including possibly diagnostic and other equipment, software and supplies at Customer locations by NetWolves. Customer agrees that safety, security and risk of loss for these products during the delivery of the Services shall be Customer responsibility. Customer will be billed for unreturned or unreasonably damaged equipment fifteen (15) days after the completion of such services or diagnostics.

3.5. Certain services could require target systems and other components including Customer internal network devices to be operational at the time of Service delivery. Customer agrees that Customer is responsible for ensuring that all necessary devices in Customer's network are operational, as required, to successfully deliver the Services. In the event any of Customer necessary devices, including Customer internal network devices, fail to perform, or cause a delay in NetWolves' response or resolution of a problem on Customer network and/or system, such delay will not count against NetWolves' performance of management services and may result in additional charges at NetWolves' then current rates for the services provided by NetWolves to assist in resolving the problem.

3.6. To provide the Services in this MNO, NetWolves requires Customer to provide certain technical information and requirements in advance of and/or during the performance of the Services. These requirements include, but are not limited, to the following items:

- Customer will provide all IP addresses, application transport requirements (if applicable), and IP network performance requirements (if applicable) associated with the solution being monitored and/or managed by NetWolves.

- Prior to the implementation date, Customer will provide circuit information, circuit numbers and network diagrams, to NetWolves for all circuits not provided by NetWolves. Details of service commitments from common carriers associated with these circuits not provided by NetWolves will also be provided.

**Customer will provide an environment that falls within the operational specification of the equipment manufacturer. The Customer is liable for any and all environmental or physical damage to CPE (Customer Premise Equipment) within the Schedule A.*

4. General

4.1. NetWolves disclaims all liability for any damages caused by the negligent acts or omissions of Customer's service providers. NetWolves will not be responsible for the failure of Customer's service providers to perform duties necessary to allow NetWolves to maintain Customer's network and/or systems as provided herein. In the event any of Customer's service providers fail to perform, or cause a delay in NetWolves' response or resolution of a problem on Customer's network and/or system, such delay will not count against NetWolves' performance of management services and may result in additional charges at NetWolves then current rates for the services provided by NetWolves to assist in resolving the problem. In the event any service provider fails to assist NetWolves as required, Customer agrees to meet with such provider to ensure compliance with NetWolves' instructions. Customer agrees to hold NetWolves harmless against any claims, losses, actions, damages, or settlements brought by Customer's service provider against NetWolves resulting from the exercise of the agency arrangements or the performance of this MNO.

4.2. NetWolves reserves the right to assign, re-assign and substitute its personnel with others having comparable qualifications at any time. NetWolves reserves the right to subcontract any or all of the Services to third parties and independent consultants ("Subcontractors").

4.3. Activities performed by NetWolves in no way creates a partnership or joint venture between NetWolves and Customer or any of the Customers service providers. All parties involved under the performance of Services hereunder will beconsidered independent contractors.

4.4. Billing for Managed Services will commence within 14 days of date when configurations are implemented and tested by NetWolves. Customer's failure to implement the necessary changes to their network and/or devices does not eliminate the Customer's contractual obligations to the services contained herein.

**If any changes are needed to the customer's network design, a charge for professional engineering services may apply and will require an updated Schedule A.*

5. Network Monitoring & Reporting Options:

MNS provides several network monitoring options for our customers to choose from to best suit their operational requirements. These different options or levels tie directly to the NetWolves NHQ categories and provide flexibility as dictated by client's business needs. All monitoring is handled 24x7x65 by our Network Command and Control (NC^2) facility located in Tampa, FL and is accessible to the customer at any time.

5.1. <u>Network Monitoring & Reporting Options:</u>

Silver Level: *NHQ categories: Availability*

Silver Level product offering provides basic up or down monitoring per circuit and/or a single device utilizing standard ICMP pings. NetWolves will ping the remote node every 60 seconds for devices, which utilize carrier services with performance Service Level Agreements (SLA) (e.g. MPLS, DIA, etc.). For infrastructure utilizing best effort WAN connectivity (e.g. commercial broadband), NetWolves will ping the monitored device every 240 seconds. If the device fails to respond after three attempts, NetWolves NC^2 receives an alert and follows the appropriate Standard Operating Procedure (SOP) assigned to that customer and circuit. If no specific SOP exists, the NC^2 will follow default customer handling procedures. Once the device is again responding to our monitoring systems for 5 consecutive minutes, the device is considered to be operating as normal. NetWolves can monitor any circuit type terminated on a device capable of and permitted via security rules to respond to ICMP ping requests. Broadband circuits may require a device in addition to the Telco provided CPE, which is capable of responding to an ICMP ping request. Customers under contract for silver monitoring receive a weekly availability report sent to an email distribution list, which has been supplied by the primary contact. This report is delivered no later than NetWolves' close of business (CoB) on the following Friday.

Gold Level: *NHQ categories: Availability, NNP, Utilization*

Gold Level product offering provides a more in-depth level of monitoring for network CPE by utilizing Simple Network Management Protocol (SNMP). This gives our Service Assurance (SA) staff the ability to monitor interface statics, CPU and memory utilization. Another major advantage of SNMP, all information being monitored is gathered locally by the device and retrieved by our polling systems on a set interval. As in our silver offering, these intervals are 60 seconds for facilities utilizing carrier services with an SLA and 240 seconds for facilities utilizing best effort services (e.g. commercial broadband, etc.). In the event that our systems fail to connect to a device after 3 attempts, they will re-attempt every 60 seconds and will be alerted as a down until connectivity is restored. In addition to availability/connectivity, interface errors and packet drops are monitored with Gold Level support. In the event that any targeted WAN interface with a supporting SLA reports 5% packet loss over a span of 5 minutes, or receives 500 errors within 5 minutes, an alert is triggered. For targeted WAN interface with no supporting SLA, alerts are triggered for 10% packet loss or 1500 errors within a span of 15 minutes. Just as in Silver Level monitoring, the NC^2 will follow the appropriate SOP for the alert. Additionally, we monitor real-time and historical utilization for all network backbone interfaces and circuits as well as round-trip response times between our management systems and each monitored device. By default, alerts are triggered when an interface reaches 90% utilization for 15 minutes and when a device's response time exceeds 2 seconds for more than 5 minutes. Gold level monitoring also includes customer web portal access. All Gold level monitored devices (NetWolves or customer provided) must be SNMP Version 2 capable and accessible from our NC^2. All non-NetWolves provided CPE requires NetWolves Service Engineering approval. NetWolves Provided Equipment or (NPE) is available for an additional charge. Customers under contract for gold monitoring will receive a weekly availability, and circuit utilization report via email to the distribution list supplied by the primary contact. This report will be delivered no later than NetWolves' CoB on the following Friday.

Platinum Level: *NHQ categories: Availability, NNP, utilization, User behavior, Traffic trending*

Platinum Level product offering provides all of the functionality of our gold level offering plus the addition of our proprietary WPP (WolfPac Platinum) monitoring platform. As described in the "Traffic Trending" & "User Behavior" sections above, the WPP provides for capture, recording, and inspection of almost everything within the traffic flows of a facility's network. The WPP platform's functionality consists of:

Security:

Vulnerability reporting via OpenVAS. Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. An OpenVAS scan can detect over 25,000 different potential security risks on a particular host. Providing a vulnerability report is a very intense exercise, requiring planning and coordination between NetWolves, the customer and potentially any 3rd parties which the client may be exchanging data with. Undertaking a vulnerability assessment with a subsequent report for a customer will be evaluated on an individual case basis.

SNMP walk via Net-SNMP. An SNMP walk allows you to detect a set of variables that are available for reading on a certain device. You can obtain a full or partial list. By analyzing the results of a network device scan obtained with an SNMP walk you can develop a list of supported Management Information Bases (MIBs) and, in this way, obtain full descriptions of variables and possible values.

Traffic Trending Apps:

NTOP: Is a network traffic probe that monitors and displays network traffic flows. Agents can use a web browser to navigate through traffic information and various views of the network's status such as:

- Sort network traffic according to many protocols
- Show network traffic sorted according to various criteria
- Display traffic statistics
- Identities of computer users
- Passively (i.e. without sending probe packets) identify the host OS
- Show IP traffic distribution among the various protocols
- Analyze IP traffic and sort it according to the source/destination
- Display IP Traffic Subnet matrix (who is talking to who?)
- Report IP protocol usage sorted by protocol type

Netflow Export: All network traffic analytics collected by the WPP can be exported to a 3rd party application in the form of Netflow. This is a feature of the FProbe application.

Network Traffic Capturing:

- PCAP creation & searching via Wireshark: Wireshark is software that "understands" the structure of different networking protocols, thus, it is able to display the encapsulation and the fields along with their meanings of different packets specified by different networking protocols. Wireshark uses PCAP to capture packets, so it can only capture the packets on the types of networks that PCAP supports.
- Real-time traffic capturing via tcpdump: tcpdump can capture and display the packet headers on a particular network interface or on all interfaces. Tcpdump can display all of the packet headers, or just the ones that match particular criteria.

Traffic Counter and Estimator via vnStat: is a console-based network traffic monitor for Linux and BSD that keeps a log of network traffic for the selected interface(s). It uses the network interface statistics provided by the kernel as the information source:

- Gathered throughput statistics persists through system reboots
- Can monitor multiple interfaces at the same time
- Several output options
  - Summary, hourly, daily, monthly, weekly, top 10 days
  - Optional image output
  - Months can be configured to follow billing period

Network Performance Apps:

Throughput testing via Iperf: is a commonly used network testing tool that can create TCP and UDP data streams and measure the throughput of a network that is carrying them. Iperf can also perform raw throughput testing via ICMP.

Management Apps:

- OoB (Out of Band) access via Broadband connection or Dial-up
- File configuration and operations system image storage & transfer via Curl: a tool for transferring data using various protocols including HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, LDAP, LDAPS, DICT, TELNET, FILE, IMAP, POP3, SMTP and RTSP.
- SYSLOG storage & searching via LogAnalyzer: is a web interface to syslog and other network event data. It provides easy browsing, analysis of real-time network events and reporting services.
- NTP via native UNIX.

** Customers under contract for platinum monitoring will receive weekly availability, and circuit utilization reports via email to the distribution list supplied by the primary contact. These reports will be delivered no later than NetWolves' CoB on the following Friday. Additionally, platinum monitored customers will receive monthly network user top-talker reports. This report will be delivered no later than NetWolves' CoB of the 10th day of the following month.*

**NOTE: Regardless of services offered in Platinum level monitoring, only one WolfPac Platinum will be deployed per individual customer facility.*

5.2. Managed Network Options:

Our dominant value add to customers is our Manage Network Services (MNS) practice. Continuing the goal of fitting solutions to the business requirements of our customers, MNS is divided into major services in addition to monitoring and reporting. These services are defined below:

- ***MNS Core Network Services****:* Like most Internet Service Providers (ISP's), NetWolves offers an entry-level management solution for customers who have simple connectivity needs. CNS includes basic functionality and a pay as you grow structure
  Silver level monitoring and reporting (Upgradeable to Gold)
  Basic Internet Access – monitoring does not include internal (intranet) connectivity status
  *Basic VPN configuration support for NPE
  All other NMO services are billable

**Basic VPN support is defined as Cisco proprietary spoke-to-spoke DMVPN configuration. At this level, NetWolves will not monitor intranet connectivity status.*

- **MNS Advanced Network Services (ANS**): The Advanced Services offering provides the next level management for clients who have more complex connectivity requirements. ANS includes:
  Gold level monitoring and reporting (Upgradeable to platinum)
  Additional weekly packet loss response time report
  Additional monthly WAN circuit utilization reporting
  Full feature set configuration support for NPE
  Up to 4 RMAC executions per calendar month not to exceed 16 NetWolves work hours
  In scope CPR (Out of scope CPR's are billable)
  All other NMO services are billable

- **MNS Enterprise Managed Services (EMS):** The NetWolves Premium MNS offering. EMS level management is targeted for large enterprise class customers with a high change rate and includes all offered services. EMS includes:
  Platinum level monitoring and reporting
  Additional monthly NC^2 ticket report*
  Quarterly Managed Services Report (QMSR) and NUM operating systems (IOS) report
  Full feature set configuration support for NPE
  Uncapped RMAC execution
  ECP execution up to 40 estimated project hours per calendar year
  Both in-scope and on demand CPR

*The NetWolves Network Command and Control (NC^2) will provide a monthly incident report, which provides a single source document outlining all service impacting tickets handled the previous month. The document details the source of initial notification, previous month list of tickets, ticket category breakdown, time to incident resolution and NC^2 performance quality scorecard.

5.3. Managed Security Options:

Continuing to offer flexibility, we have extended the 3-tier model from MNS to the managed security bundles as well.

- **MSS Core Perimeter Services**: NetWolves offers an entry-level security solution for customers who require simple solutions. CPS includes basic functionality targeted for content filtering and a compliancy certified firewall. This product will be delivered via the Meraki MX platform. CPS includes:
  - MNS Gold level monitoring and reporting
  - Aggregated Content filtering
  - Monthly web usage report
  - VPN Tunneling (Site to Site)
  - 3G/4G Failover
  - Up to 4 RMAC executions per calendar month not to exceed 16 NetWolves work hours
  - In scope CPR (Out of scope CPR's are billable)
  - All other MNO services are billable

- **MSS Advanced Perimeter Services:** The APS offering provides the next level of services offered to customers who have more complex security requirements. These services will be delivered utilizing Palo Alto's next generation Firewall Appliance. APS includes:
  - MNS Platinum Monitoring and Reporting
  - User based Content Filtering
  - Application Management
  - Support for up to 10 Virtual Firewalls
  - Data Loss Protection
  - MSS Reporting (TBD)
  - Up to 4 RMAC Executions per Calendar Month not to exceed 16 estimated NetWolves work hours
  - In scope CPR (Out of scope CPR's are billable)
  - All Other MNO Services are billable

- **MSS Enterprise Perimeter Services**: Building on the APS offering, EPS includes our most comprehensive bundle of security products and services. These services will be delivered utilizing Palo Alto's next generation Firewall Appliance. The EPS bundle includes:
  - MNS Platinum Monitoring and Reporting
  - User Based Content Filtering
  - Application Management
  - Support for unlimited Virtual Firewalls limited to the capability of the hardware
  - Data Loss Protection/Prevention
  - IPS/IDS services
  - SIEM services provided through IBM QRadar. Log retention of 60 days*.
  - Perimeter Based Anti-Virus & Anti-Spyware
  - MSS Reporting (TBD)
  - Uncapped RMAC Execution
  - Both In-scope and On Demand CPR
  - QMSR Execution

** A monthly true-up of the EPS and/or FPM limit will be optional to the customer after analysis of the monthly Managed SIEM report. If customer decides to increase EPS and FPM limits additional true-up charges will apply. If the customer does not choose to increase EPS and/or FPM based to this data, they will be subject to rate limiting. A monthly true-up of the EPS and FPM limit will be optional to the customer after analysis of the monthly Managed SIEM report. If customer decides to increase EPS and FPM limits additional true-up charges will apply.*

5.4. Traffic Optimization Services Options:

The Managed Network Services (MNS) practice provides three levels of management for our client's Traffic Optimization Services (TOS), similar to the Managed Network Options listed previously. At this time, NetWolves support is only available on Riverbed's Steelhead platform. Services included per each tier are defined below.

- **MNS Advanced Traffic Optimization (ATO):** The Advanced offering provides the next level management for clients who have more complex WAN architectures and requirements. ATO requires clearly defined management goals and includes:
  - Active monitoring of the Traffic Optimization infrastructure (Gold Level Equivalent)
  - Monthly optimized throughput report (exampled below)
  - Additional monthly review of bandwidth consumption and suggested policy changes (as RMAC)
  - Optimization support for all applications excluding those with any authentication requirements (i.e. MAPI, SMB-3, etc.)
  - Up to 4 RMAC executions per calendar month not to exceed 16 NetWolves work hours
  - In scope CPR (Out of scope CPR's are billable)
  - All other Traffic Optimization Services are billable

- M**NS Enterprise Traffic Optimization (ETO):** NetWolves' Premium level of Traffic Optimization Services. ETO level management is targeted for large enterprise class customers with multiple campus and satellite offices along with significant bandwidth utilization benefiting from an optimized approach. ETO includes all previously listed services as well as:
  - Monthly reports to include:
    Optimized throughput
    Bandwidth optimized (exampled below)
    Traffic Summary (exampled below)
  - Additional monthly NC² ticket report*
  - Active monitoring of the Traffic Optimization infrastructure (Gold Level Equivalent)
  - Quarterly Managed Services Report (QMSR) and NUM operating systems (IOS) report
  - Active Directory (AD) acceleration and integration
  - SSL optimization
  - QoS
  - "Interceptor" deployment and management for scalability of capacity
  - Path Selection and Prioritization
  - Uncapped RMAC execution
  - Both in-scope and on demand CPR

5.5. <u>WiFi Managed Network Options</u>:

The Managed Network Services (MNS) practice also provides two levels of management for our client's Wi-Fi or WLAN Infrastructure under Managed LAN Services (MLS), which differ slightly from the Managed Network Options listed previously. At this time, NetWolves support is only available on Meraki based Wireless Deployments. Services included per each tier are defined below. It is important to note our area of demarcation with this service. NetWolves will ensure the functionality of all services listed below up to the access point itself. Our operations team will not troubleshoot end user devices (i.e. Laptops, iPads, etc.) outside of providing login configurations/parameters.

- **MLS Advanced Wireless Services (AWS**): The Advanced Services offering provides the next level management for clients who have more complex campus WiFi requirements. ASW requires that all wireless equipment to be moved into the NetWolves Dashboard and includes:
  - Active monitoring of the health of the WiFi infrastructure (Gold Level Equivalent)
  - Weekly summary reports (exampled below)
  - Additional monthly review of bandwidth consumption and suggested policy changes (as RMAC)
  - Quarterly PCI compliance reports
  - Configuration of SSIDs with shared-secret pass-phrases and rotation based upon client security policies (as RMAC)
  - Configuration support for basic Guest Access networks and splash pages (as RMAC)
  - Limited feature set configuration support for deploying additional Access Points including content filtering, and traffic shaping/QoS (Radius/AD Authentication or "Paid" Guest Networks not supported)
  - Up to 4 RMAC executions per calendar month not to exceed 16 NetWolves work hours
  - In scope CPR (Out of scope CPR's are billable)
  - All other Wireless Services are billable

- **MLS Enterprise Wireless Services (EWS**): The NetWolves Premium WiFi offering. ESW level management is targeted for large enterprise class customers with multiple campus WLANs nationally as well as a high change rate and includes all previously listed services as well as:
  - Customer may request monthly reports on:
    Real-time Heat Maps and AP location specific performance (exampled below – customer CAD/Floor plan images required)
    Full reporting of clients and client activity
    PCI Reporting
  - Additional monthly NC² ticket report*
  - Quarterly Managed Services Report (QMSR) and NUM operating systems (IOS) report
  - Full feature set configuration support for deploying additional Access Points as well as enterprise Authentication Methods (SSO) supported if client's internal authentication mechanism is compatible with NetWolves Wireless Solution
  - Configuration of advanced Guest Network options, such as "Paid Access" and analysis of guest conversion, return rate and loyalty metrics of guests
  - Uncapped RMAC execution
  - Both in-scope and on demand CPR

**The NetWolves Network Command and Control (NC²) will provide a monthly incident report, which provides a single source document outlining all service impacting tickets handled the previous month. The document details the source of initial notification, previous month list of tickets, ticket category breakdown, and time to incident resolution and NC² performance quality scorecard.*

5.6. <u>Managed Software Defined – Wide Area Networking (MSD-WAN):</u>

An SD-WAN decouples the control and management aspects of a Wide Area Network from the underlying physical network (data or network plane) infrastructure. This separation of the 'control plane' from the 'network plane' allows organizations to architect high performance WAN services utilizing lower cost broadband Internet services. The abstraction of a management layer from the specific configurations of network equipment serves to simplify the effort and resources necessary to maintain the WAN, as well as providing for automated dynamic adjustments of network resources in response to any performance issues which may occur.

- **MSD-WAN Core** utilizes BigLeaf Appliances to overlay basic SD-WAN functionality onto existing customer infrastructure. This a cost-effective entry point to gain the benefits of SD-WAN without a more involved change process. However, there are significant limitations to what the BigLeaf solution provides in the way of traditional routing and security functionality, which require existing infrastructure or additional hardware to be a full-service solution. BigLeaf SD-WAN provides a plug and play SD-WAN solution with direct access to major cloud providers for redundant connectivity that prioritizes cloud traffic. Each BigLeaf router comes pre-configured and tested, installable with a simple IP swap, minimizing risk during setup. Customer traffic is encapsulated within tunnels that connect from on-premises router, running across multiple ISP paths, to core gateway clusters. These tunnels efficiently and reliably move traffic to and from the core of the Internet, while providing an adaptation system with end-to-end visibility and control of each circuit.

- **MSD-WAN Complete** leverages the Meraki SD-WAN solution offering a lower TCO overall and is ideal for customers who are in a position to do a complete technology infrastructure refresh, looking to 'rip and replace' legacy technology, or planning to transition their environment to an enterprise grade WAN. The Meraki MX platform allow for rapid deployment and scalability for networks which utilize more common applications, such as Video or Voice over IP, and simply need the capability to secure and prioritize those types of traffic. Meraki's SD-WAN is a new approach to network connectivity that lowers operational costs and improves resource usage for multi-site deployments, allowing network administrators to use bandwidth more efficiently and ensure the highest possible level of performance for critical applications without sacrificing security or data privacy.

- **MSD-WAN Advanced** leverages Riverbed's SteelConnect for service delivery. SteelConnect is a complete SD-WAN system for securely connecting users and the business to the applications they need, wherever they reside on a remote LAN, in a datacenter, or in the cloud. SteelConnect offers: business aligned orchestration for fast, agile, and secure application delivery; and unique cloud-centric workflow, easy menu-driven network design of sites, zones, uplinks, and rules, and centralized, business intent-based policy management for ease of use and greater business agility.

- **MSD-WAN Enterprise** is NetWolves' most robust and comprehensive SD-WAN solution, offering the highest level of support and customization for a client environment. Utilizing the proprietary WolfPac™ Virtual Services Engine (VSE), Enterprise provides an extremely flexible, high performance, feature rich solution to meet any customer need. Whereas a single vendor solution generally offers peak performance in only one, the VSE takes a 'best in class' approach to services that make up the components of a complete SD-WAN solution. The VSE virtualizes and actives the best technology for the specific aspects of SD-WAN, or to meet a given customers unique need.

- **SECURE MSD-WAN Complete** – Meraki MX: VasoTechnology delivers on-premise Secure SD-WAN via the Meraki MX Platform providing powerful features at a lower TCO for customers with less complex needs. The Meraki MX platform delivers next generation security and SD-WAN in single appliance. With Meraki Secure SD-WAN, remote sites are connected over low-cost Internet links secured by AutoVPN. Network reliability is provided through multiple uplinks with load balancing capabilities, intelligent path control, and automatic failover. Security settings are simple to synchronize across thousands of sites.

  Secure MSD-WAN Complete Technical Summary
  Up to 2 WAN uplinks; integrated cellular modem available on some models

  - Any type of Internet Access circuit
  - High Availability deployment (Active/Standby)
  - Intelligent Path Control
  - QoS and Bandwidth Management
  - Flexible Load Balancing
  - Basic Remote Access VPN
  - VPN WAN Topologies:
  - Spoke and Hub
  - Full Mesh
  - Basic Networking Services:
  - DHCP Server and Relay
  - NAT
  - Static Routing
  - Basic Layer 2 and Layer 3 Switching
  - VLAN support
  - Integrated NGFW Security:
  - Application control
  - Malware Protection
  - Web Filtering
  - Intrusion Prevention and Detection
  - Group-based Security Policy

Secure MSD-WAN Complete Managed Services Summary

- SRM2-S Web-based customer portal
- Network performance statistics with data retention of up to a year.
- Meraki Web-based Portal
- Traffic Analytics
- Top Clients
- Top Applications
- Top Blocked Sites
- Security Analytics
- Top Threats
- Threat Map
- Traffic and Security Analytics data retention for up to 30 days.

VasoTechnology will alert on the following events:

- When appliance goes offline (via SRM2-S alert)
- Circuit packet loss exceeds thresholds (via SRM2-S alert)
- Circuit latency exceeds thresholds (via SRM2-S alert)
- A VPN connection goes down (via Meraki email to NC2)
- IP Conflict is detected (via Meraki email to NC2)
- A Rogue DHCP server is detected (via Meraki email to NC2)
- Malicious File Detected (via Meraki email to NC2)
- A warm spare failover occurs (via Meraki email to NC2)
- Service Level Agreement and alarm thresholds are dependent on circuit types. Refer to the NC2 SOP.
- Up to 4 RMAC executions per calendar month not to exceed 16 VasoTechnology work hours
- In-scope Critical Problem Review (CPR) defined as a critical production outage affecting multiple customer sites for durations of 2 hours or more

Meraki Secure SD-WAN Architecture Overview:

The Meraki's SD-WAN approach to network connectivity lowers operational costs and improves resource usage for multi-site deployments, allowing network administrators to use bandwidth more efficiently and ensure the highest possible level of performance for critical applications without sacrificing security or data privacy.

Features at a glance:
Transport Independence

- Easy-to-configure IPsec overlay using Meraki Auto VPN
- Traffic distribution over multiple pathways (Internet, cellular, MPLS) with built-in load balancing and automatic failover capabilities application optimization
- Centralized network visibility and control
- QoS and bandwidth management with Meraki traffic shaping
  Intelligent Path Control
- Policy-based routing (PbR) functionality allows administrators to assign traffic to a particular VPN path based on criteria such as traffic protocol, source, destination, or application.
- Dynamic path selection allows administrators to set performance thresholds for different types of traffic, in order to ensure that critical applications and data transfers always use the best path based on the loss, latency, and jitter over the available VPN tunnels.
  Secure Connectivity
- Intuitive, scalable VPN solution to connect remote sites with ease (AutoVPN)
- AES encryption to ensure data privacy

• SECURE MSD-WAN Advanced - Fortinet FortiGate

VasoTechnology delivers on-premise Secure MSD-WAN Advanced for clients who have more complex requirements. In addition to providing standard SD-WAN capabilities, FortiGate Secure SD-WAN goes a step further as the market's first solution that eliminates the need for costly multidevice standalone security, while also simplifying infrastructure architecture. With this product, the NGFW (Next Generation Firewall) is not simply an add on. It is an integrated full security stack that sits on the Branch Edge, mitigating the additional bandwidth consumption of third-party security options while reducing the possibility of bottlenecks. Utilizing security processors to provide selective acceleration, and parallel path processing, the use of a single device increases performance and lowers hardware footprint while remaining scalable. Traffic visibility provided by built in security features result in far more granular control than independent solutions offer, both in terms of traffic handling and application or user-based rulesets.

Secure MSD-WAN Advanced Technical Summary

- Multiple Wan uplinks limited only by model selection
- Any type of access circuits including Internet Access Circuits, MPLS and Metro-E
- Supports High Availability deployment
- Intelligent Path Control
- QoS and Bandwidth Management
- Flexible Load Balancing
- Advance Remote Access VPN with available VPN Client and flexible authentication methods
- VPN WAN Topologies:
- Spoke and Hub
- Dynamic multipoint VPN
- Full mesh VPN
- Advanced Networking Services:
- DHCP Server and Relay
- NAT and SNAT
- Full OSPF and BGP Support
- Advanced Layer 2 and Layer 3 Switching
- Link Aggregation Protocol
- First Hop Redundancy Protocol
- Rapid Spanning Tree Protocol
- Advanced Integrated NGFW Security:
- Granular Application control (5K plus apps)
- Granular Malware Protection
- Granular Web Filtering: User-based and Group-based
- Intrusion Prevention and Detection
- User-based and Group-based Security Policy
- Additional product feature, e.g. through license add-on may be supported per individual case basis.

Secure SD-WAN Advanced Managed Services Summary:

- SRM^2-S Web-based customer portal
  - VasoTechnology leverages SRM2-S for network performance statistics with data retention of up to a year.

- FortiAnalyzer Web-based Portal
  - FortiAnalyzer Web Portal provides customers with enhanced Traffic Analytics, Security Analytics and On-demand Report Templates.
  - Traffic Analytics
    - Top Sources and Destinations
    - Top Country and Region
    - Policy Hits
    - DNS Logs
    - Top Applications and Websites
    - Top Cloud Applications
    - Top Cloud Users
    - Top Website Domains
    - Top Website Categories
    - Top Browsing Users
    - Security Analytics
    - Top Threats
    - Threat Maps
    - System Logs

- Antivirus Logs
- Intrusion Prevention Logs
- Application Control Logs
- Web Filter Logs
- DNS Logs
- Event logs e.g. SD-WAN Health Check Logs

  - Data retention is dependent on subscription, the default is based on number of devices in the environment estimated for up to 6 months analytical data and 6 months archive. However, this is only an estimate, actual retention period will be dependent on the number of logs devices generate based on number of users. Additional storage can be purchased in increments of 1GB Logs/Day with 500GB Storage.

- Proactive alerts

  VasoTechnology will alert on the following events:

  - When appliance goes offline (via SRM2-S alert)
  - Circuit packet loss exceeds thresholds (via SRM2-S alert)
  - Circuit latency exceeds thresholds (via SRM2-S alert)
  - A VPN connection goes down (FortiAnalyzer email to NC2)
  - An IP Conflict is detected (FortiAnalyzer email to NC2)
  - A Rogue DHCP server is detected (FortiAnalyzer email to NC2)
  - Malicious file detected (FortiAnalyzer email to NC2)
  - A warm spare failover occurs (FortiAnalyzer email to NC2)
  - Botnet communication detected via (FortiAnalyzer email to NC2)
  - Error and critical level events (FortiAnalyzer email to NC2)

  *Service Level Agreement and alarm thresholds are dependent on circuit types. Refer to the NC2 SOP.

- Up to 4 RMAC executions per calendar month not to exceed 16 VasoTechnology work hours

- In-scope Critical Problem Review (CPR) defined as a critical production outage affecting multiple customer sites for durations of 2 hours or more

5.7. <u>Telecommunications Carrier Management (TCM) Options:</u>

- Customer owned non-SLA services (i.e. Broadband): Product provides for a customer to bring a non-SLA circuit not provided by NetWolves into the MNO product set and allows NetWolves to act on the client’s behalf for trouble shooting and restoration of non-SLA circuits.
- Customer owned SLA services (Example T-Carrier) Product provides for a customer to bring a SLA circuit, not provided by NetWolves, into the MNO product set and allows NetWolves to act on the client’s behalf for trouble shooting and restoration of SLA circuits.
- This product requires a Letter of Agency (LOA) from the existing telecommunications carrier that authorizes NetWolves to take incident management action on the customer’s behalf. Additionally, the client will need to supply a TCM checklist containing all technical information and points of contact to manage the service and requires NetWolves engineering approval.