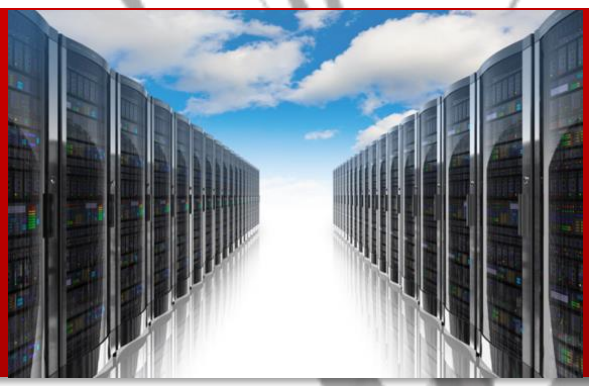


NetWolves Managed Services

[Sample Customer]

Quarterly Managed Services Report

[Date]

Contents

Executive Summary

Quarterly Managed Services Review (QMSR)

The analysis and report that delivers trended quality network and services information about the customer, highlighting key activities, metrics and trends in order to provide conclusions and recommendations. The foundation of the QMSR is to measure the holistic quality of a network (NHQ) by analyzing and reporting on the following areas: Network Availability, Network Node Performance, Utilization, User Behavior, and Traffic Trending. By aggregating these metrics, NetWolves can provide true insight into your network operations infrastructure and demonstrate the benefits of using our value added services.

Customer X Education NetWolves Partnership

Background/Services Summary:

Having partnered with Customer X (formerly Customer X) since July of 2009, NetWolves understands the critical value of network operations to the success of Customer X' business model. NetWolves began its relationship with Customer X on a contract basis to complete a Telecom Site Assessment and an Information Technology Review. The relationship soon evolved to network aggregation services and basic monitoring. Customer X' current services include a monitored and managed dual Service Provider, MPLS VPN WAN intranet centralized network with direct internet access located at the Customer X Data Center data center. Currently, there are 26 campus locations and 3 office locations. The primary MPLS consists of 20M circuits at 21 campus locations, 40M circuits at 4 campus locations and 100M at the Aurora campus and the office locations. The primary network includes two – 1G host circuits at the data center. The back-up MPLS consists of 1.5M T1 circuits at the campus locations, 6M circuits at the office locations and a 50M host circuit at the data center. NetWolves provides a 1G DIA circuit at the data center. NetWolves monitoring and management extends to all network devices, providing alerting and pro-active break fix to facilitate quick problem resolution.

Current Initiatives:

NetWolves is pleased with the productive meetings in Tampa the last week in April. Customer X shared the 2015 security initiatives and our teams reviewed where NetWolves can assist. NetWolves is excited about our Managed Security Services proposal, providing both an "eyes on" and "eyes off" option. Backed by our IBM partnership, the proposed solution includes Live Security Monitoring via IBM's Secure Operations Center, Threat Analyst Escalation and Auto alerting of health and availability of your devices. This service will be fully integrated into your current alert and reporting processes, taking advantage of existing procedures and NetWolves expertise and assistance to save you time and money.

Additionally, all open items were reviewed and several key decisions were made on next steps to improve resiliency in the event of an outage.

- *AR Routing:* Our teams successfully implemented the ASR routing change to full routing, which will improve failover performance.
- *BGP Time Thresholds:* The decision was made to proceed with testing the reduction of BGP timer thresholds to 15/45.
    - Ocala Nursing was chosen as the test location.
    - Orders have been placed with the underlying facility providers and NetWolves anticipates the hot cut can be scheduled in late July.
- *Performance Based Routing (PfR):*
    - NetWolves Engineering is finalizing the lab to complete necessary testing

- *Network Upgrade:* NetWolves installed a burstable 20M DIA circuit at Aurora to facilitate Customer X' Disaster Recovery roll out at this location.
- *Maintenance Alerts:* To enhance communications, Customer X and NetWolves finalized an updated alert distribution creating two distribution sets, which allows alerts to be sent to different groups within Customer X based on level of severity.

Additional items the NetWolves and Customer X teams are working on include:

- Campus Connect: Customer X has advised that the next 4 sites have been determined – Fargo, Eagan, Green Bay and Aurora
    - Fargo and Eagan – NetWolves proposed an MPLS upgrade to 40M each
    - Green Bay – NetWolves proposed a VPN replacement to 50M MPLS
    - Aurora – No change required (service upgraded to 100M in February 2015)
- VPN site conversions to CenturyLink MPLS where available.
    - Appleton and Green Bay – Proposed
    - Romeoville – Order to be held till October to offset ETL for Bismarck MPLS circuit to be cancelled when campus closes in November.
- Ocala Move – Targeted for May 2016

Future Potential Projects:

- As NetWolves understand critical nature of traffic and the growing need of bandwidth presentation, NetWolves advises deploying Riverbed SteelHead appliance for WAN optimization. NetWolves has had success with several customers and increased bandwidth availability in excess of 30%. This deployment will allow the existing primary circuit to remain in place without the need to increase operational expenses for the primary circuit.

- With Customer X' growing Campus Connect requirements, NetWolves suggests increasing the bandwidth of the back-up MPLS network to ensure network resiliency in the event of any incident on the primary MPLS network. NetWolves is reviewing alternate carrier options to meet this objective.

Customer X Education Q2 Highlights

Network Holistic Quality (NHQ)

Definition: NetWolves measures the holistic quality of a network (NHQ) by sampling and/or reporting on the following categories:

- Availability
- Network Node Performance (NNP)
- Utilization
- User behavior
- Traffic trending

By aggregating these metrics, we can provide our customers with true insight into their infrastructures and show value add in our services.

Availability: measured at the device level by providing a percentage of time that NetWolves' monitoring systems are accessible from NetWolves SRM2-S Monitoring Environment

Facility Availability: measured as the uptime average percentage of a specific location taking into account the solution design (failover possibility)

Included below are the major highlights of the NHQ analysis, with a summary of availability, CPU/memory utilization, and the Engineering Roadmap recommendations with details following in the body of the report.

Availability Summary

Type	Availability Percentage	Impact Duration (On Failover if Applicable)
Facility MPLS Availability	99.9992%	~16 minutes
Internet Availability	100.00%	0 minutes
Facility Switch Availability	99.999%	~16 minutes
Facility Core Switch Availability	99.999%	~16 minutes

CPU Utilization Summary

Node	Average CPU Load	Peak CPU Load
Customer X-greenbay-CS-1-90302290	38.00%	49.00%
Customer X-romeovil-CS-1-90302300	38.00%	42.00%
Customer X-wausau-CS-1-90302303	35.00%	55.00%
Customer X-Customer X Data Center-SW-12-200006001	34.00%	42.00%
Customer X-Customer X Data Center-SW-1-200006001	31.00%	43.00%

Memory Utilization Summary

Node	Average Percent Memory Used
Customer X-maitland-VR-1-90302296	82.00%
Customer X-fortmyer-VR-1-90302289	73.00%
Customer X-aurora-VR-1-90302284	71.00%
Customer X-moorhead-VR-1-90302295	68.00%
Customer X-mankato-VR-1-90302294	67.00%

Application Utilization Summary

Application	Percentage	Ingress Traffic in Tbytes
World Wide Web HTTP (80)	25.97%	74.4
Microsoft-DS (445)	24.36%	69.6
http protocol over TLS/SSL (443)	15.07%	43.2
CAPWAP Data Protocol (5247)	14.07%	39.6
Unmonitored traffic	8.41%	24

Roadmap

Engineering Services Review:

The NetWolves Engineering Team has started seeing positive results of several enhancements in our standard operating procedures which were made last quarter to support increased reporting and review processes. In addition, our team has worked with Customer X on additional enhancements. One such enhancement was to route incoming internet traffic via the Nitel circuit to avoid additional billing on the Customer X Data Center 200M burstable circuit. Additionally, other enhancements included targeting increasing WAN availability and faster convergence.

Engineering Services is proud to once again achieve five 9's for facility availability. This marks the third quarter where this key metric was reached and was achievable through partnership and continued cooperation between NetWolves and Customer X.

NetWolves Engineering Services strives for to continuous improvement in all network solutions, and as such, we have the following recommendations:

- NetWolves understands the importance of network and facility availability. Last quarter NetWolves Engineering Services recommended reducing the BGP (Border Gateway Protocol) timer to 15/45 in an effort to reduce route flapping in the event of packet loss on the circuit. We are working with the carriers to accommodate the new timers and working on scheduling the hot cuts for both carriers. Once complete, facility availability is expected to increase as the failover timer will be greatly decreased.

- The NetWolves Engineering Services team has also recommended implementing Performance Routing (PfR) to reduce failover and convergence time for all voice traffic at the Aurora location to provide greater stability for the call center. The NetWolves engineering team is working on the proof of concept LAB for PfR delivery.

- The NetWolves engineering team would recommend deploying Riverbed WAN optimizer to avoid high bandwidth consumption and full utilization of the circuits. The average campus' receive utilization is approximately 2mb/s. In the event the primary Ethernet MPLS circuit fails, the backup T1 (1.5mb) is unable to sustain the full load. Allowing NetWolves Engineering Services to deploy and manage WAN optimization will allow for up to 80% reduction in certain traffic types allowing the backup circuit to take the full campus load in the event of failure resulting in less end user impact.

- As identified in the last QMSR, and again this quarter, the secondary circuit at each location is not capable of supporting growing business critical applications and services in the event of a primary circuit failure. NetWolves recommends upgrading each secondary circuit to provide proportional balance between the primary and secondary circuits or deployment of WAN Optimization.

- Across many campuses, core and access switches are beginning to reach their end-of-life dates and are unable to support the current load evident in spikes in CPU and Memory. Engineering Services recommends replacing/upgrading these switches to the current Cisco model. Building on this, NetWolves also recommends beginning a LAN refresh project targeting critical locations in need of dual core switches to ensure maximum availability.

- As of October 31, 2011 Cisco announced the EOS dates for the ISR G1 2801 and 2821 routers. These devices will reach their end of support on October 31, 2016. Currently, there are 69 Cisco 2821 routers, 1 2801 router, 2 3825 routers, and 2 3845 routers in production. NetWolves Engineering Services recommends upgrading End-of-Support routers to the current Cisco ISR G2 Platform for mission critical locations.

- NetWolves engineering team has been reviewing a weekly Packet Loss Tool report to identify any potential design or configuration issues. We have worked proactively with the NC2 to open tickets with facility providers and work towards resolution to reduce further impact to the business and end users.

Managed Services Review:

Monitoring and Reporting Services Review:

Starting in Q2 2015, the NetWolves Business Analyst and Engineering Services teams will work to provide an additional weekly check on the health and quality of the WAN environment utilizing the WolfPac Platinum Appliances deployed at each location. This analysis will investigate interconnectivity issues between remote locations and the Data Center.

In the event a location has an excess of 0.05% packet loss from the Data Center to the remote location an analysis will be performed by both the Business Analyst and Engineering Services teams.

Tasks Performed by Business Analyst:

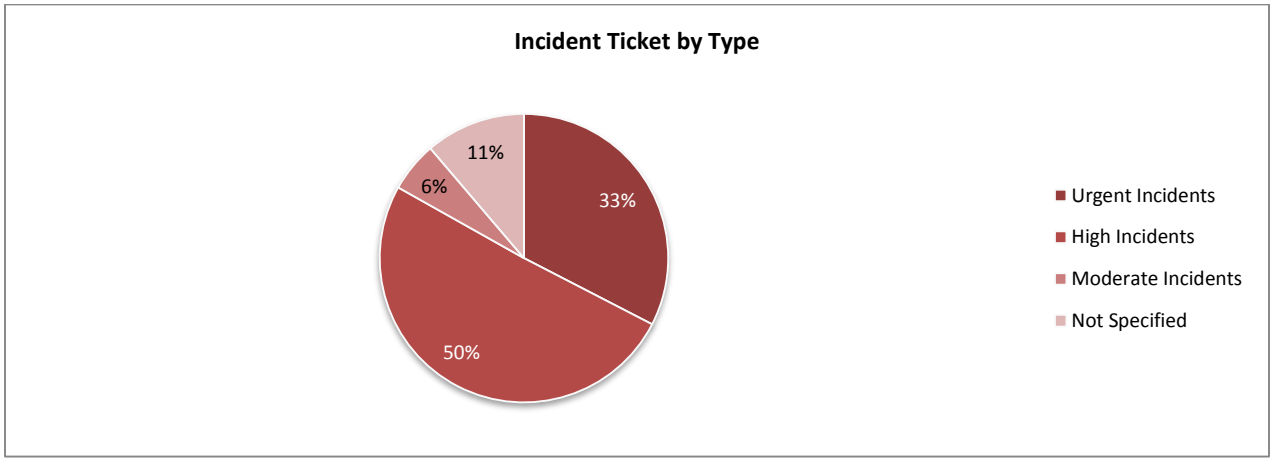
1. Review Weekly Packet Loss report by 10am each Monday
2. Identify any location in which the packet loss is unusually high for the period
3. Provide Engineering Services high level analyses for locations with unusually high packet loss
    a. Business Analyst will search for Incident and RMAC tickets and provide findings to Engineering Services
    b. Business Analyst will provide identify time/date and duration of packet loss utilizing SRM2-S and provide findings to Engineering Services

Tasks Performed by Engineering Services:

Ticket Management Review:

Over the course of Q2 2015, 89 incident tickets were.

Incident Severity	Total
Urgent Incidents	29
High Incidents	45
Moderate Incidents	5
Not Specified	10



Ticket Type	Total
RMAC	3
ECP	0
CPR	0

NetWolves Network Holistic Quality

Network Node Performance

Network Node Performance (NNP) – information and metrics about the operational resources of a specific node which are captured and recorded.
(See exhibit E for details)

Availability

Definition: NetWolves measures the holistic quality of a network (NHQ) by sampling and/or reporting on the following categories:

- Availability
- Network Node Performance (NNP)
- Utilization
- User behavior
- Traffic trending

By aggregating these metrics, we can provide our customers with true insight into their infrastructures and show value add in our services.

Availability – measured at the device level by providing a percentage of time that NetWolves' monitoring systems are accessible from NetWolves SRM^2-S Monitoring Environment.

Type	Availability Percentage	Impact Duration (On Failover if Applicable)
Facility MPLS Availability	99.9992%	~16 minutes
Internet Availability	100.00%	0 minutes
Facility Switch Availability	99.999%	~16 minutes
Facility Core Switch Availability	99.999%	~16 minutes

Taking into account the NetWolves solution with automatic failover and removing facility power loss, the adjusted WAN availability increases to **99.999%.** During this quarter, a total of 937 minutes of power loss were experienced enterprise wide.

Location	Outage Duration (Business Minutes)	Issue
Oakbrook	309 minutes	Facility power outage
Fargo	292 minutes	190 minutes due to UPS replacement
Rockford	156 minutes	Facility power outage
New Port Richey	136 minutes	Facility power outage
Wausau	29 minutes	Facility power outage
Land O Lakes	15 minutes	Facility power outage

(See Exhibit A for Details)

Facility Availability: measured as the uptime average percentage of a specific location taking into account the solution design (failover possibility)

WAN availability is calculated taking into account for automatic failover and failback. In the event a primary MPLS path fails, traffic automatically fails over to the secondary path using the default BGP timers. Downtime reflects the impact to the location where both the primary and secondary MPLS path is unusable. The majority of this time is due to a convergence required by the BGP protocol to recognize the primary path is unavailable.

Impact Duration: (On Failover) reflects the total time a location has utilized the secondary MPLS path. In all cases, the secondary has significantly less available bandwidth than the primary path. During each failover occurrence, the secondary path did not become saturated causing greater impact to the location or reduced user experience.

Least Available MPLS Router:

Device	Availability Percentage
Customer X-ocala2-MR-1-90302308	99.193%
Customer X-moorhead-MR-1-90302295	99.956%
Customer X-fargo-MR-1-90302291	99.956%
Customer X-rockford-MR-1-90302299	99.957%

Least Available LAN Switches:

Each locations core switch is monitored for availability every 60 seconds by SRM^2-S. The locations with the least available are listed above.

Device	Availability Percentage
Customer X-fortmyer-SW-1-90302289	99.996%
Customer X-Customer X Data Center-SW-4-200006001	99.999%

Utilization

Utilization – primarily based on WAN circuit utilization as this is almost always the throughput bottleneck of a network. Even so, all primary transport path or "Backbone" interfaces will be monitored by default for NetWolves' MNS customers. The below charts detailing utilization are limited to the Customer X defined business hours: Monday through Friday 6am -11pm
(See exhibit C for details)

Top 10 Circuit Utilization

- Average circuit utilization for last quarter looks normal and at this point NetWolves observers no issue with circuit utilization.

Device	Average Receive
Customer X-oakbrook-MR-1-90302309	27.06%
Customer X-twomarke-MR-1-85556374	20.92%
Customer X-brandon-MR-1-90302610	17.84%
Customer X-twinciti-MR-1-90302306	17.69%
Customer X-romeovil-MR-1-90302300	17.14%
Customer X-brooklyn-MR-1-90302286	16.64%
Customer X-mankato-MR-1-90302294	16.02%
Customer X-blaine-MR-1-90302305	15.23%
Customer X-deltak-MR-1-200008745	15.19%
Customer X-rockford-MR-1-90302299	15.07%

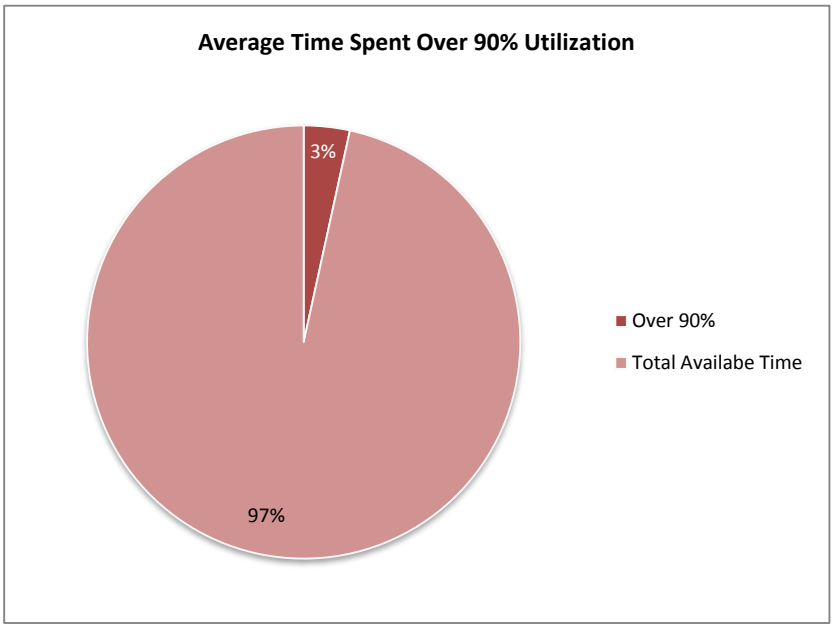
Device	Average Transmit
Customer X-Customer X Data Center-FW-2-200006001	14.18%

(See Exhibit C for Details)

Customer X-aurora-MR-1-90302284	11.95%
Customer X-ocala2-MR-1-90302308	9.43%
Customer X-Customer X Data Center-IR-2-200006001	9.27%
Customer X-oakbrook-MR-1-90302309	8.91%
Customer X-maitland-MR-1-90302296	7.97%
Customer X-brooklyn-MR-1-90302286	7.01%
Customer X-Customer X Data Center-MR-1-200006001	6.78%
Customer X-Customer X Data Center-FW-4-200006001	6.49%
Customer X-brandon-MR-1-90302610	6.48%

A detailed review was performed for all primary MPLS circuits for the month of June to determine Engineering Service recommendations. Based on the findings, the average primary MPLS (CenturyLink) circuit exceeds 90% utilization for approximately 3% of the time or 195 minutes. Additionally, utilization exceeded 80% for 390 minutes and 70% for 735 minutes enterprise wide.

The NetWolves engineering team would recommend deploying Riverbed WAN optimizer to avoid high bandwidth consumption and full utilization of circuit. The average campus' receive utilization is approximately 2mb/s. In the event the primary Ethernet MPLS circuit fails, the backup T1 (1.5mb) is unable to sustain the full load. Allowing NetWolves Engineering Services to deploy and manage WAN optimization will allow for up to 80% reduction in certain traffic types allowing the backup circuit to take the full campus load in the event of failure resulting in less end user impact.



Top 5 Device CPU Utilization

Node	Average CPU Load	Peak CPU Load
Customer X-greenbay-CS-1-90302290	38.00%	49.00%
Customer X-romeovil-CS-1-90302300	38.00%	42.00%
Customer X-wausau-CS-1-90302303	35.00%	55.00%
Customer X-Customer X Data Center-SW-12-200006001	34.00%	42.00%
Customer X-Customer X Data Center-SW-1-200006001	31.00%	43.00%

(See Exhibit B for Details)

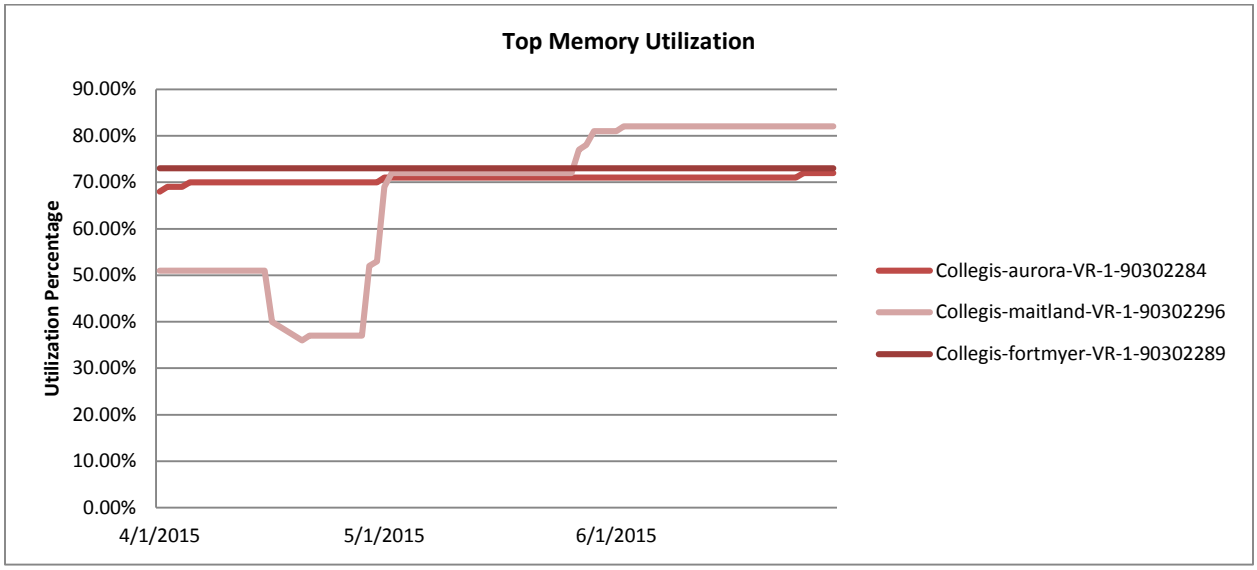
Top 5 Memory Utilization

Node	Average Percent Memory Used
Customer X-maitland-VR-1-90302296	82.00%
Customer X-fortmyer-VR-1-90302289	73.00%
Customer X-aurora-VR-1-90302284	71.00%
Customer X-moorhead-VR-1-90302295	68.00%
Customer X-mankato-VR-1-90302294	67.00%

(See Exhibit B for Details)

An analysis was performed on the three (3) below routers to determine the high memory utilization.

- Customer X-maitland-VR-1-90302296: Beginning in late May, this device's utilization spiked over 80% for the first time during Q2 and has held at this level for the remainder of the quarter
- Both Customer X-fortmyer-VR-1-90302289 and Customer X-aurora-VR-1-90302284 hold steady around 70% utilization with no spikes.



User Behavior and Traffic Trending

User behavior as defined by NetWolves is what a device on the network is accessing over the WAN. Our ability to monitor and report this metric is accomplished by implementing our proprietary device named "WolfPac Platinum" (WPP) as additional CPE. This device can be deployed in one of three ways:

> **In-line:** The WPP appliance is placed physically in-line between the NetWolves provided facility edge router and the LAN layer 2/3 device, thus forcing all traffic between the LAN and the facility edge through the WPP. In this deployment style, the WPP is configured for bypass, which allows traffic to flow in the event of a power failure.
>
> **Span:** The WPP appliance is physically connected to the facility main/Core layer 2/3 device. This deployment method is dependent on span capabilities in the core.
>
> **VLAN Bridge:** In instances where the core device is not span capable, the WPP appliance can act as a bridge between two VLAN's, thus again forcing all traffic between the LAN and the facility edge through the WPP.

For the Customer X solution, NetWolves has deployed all WPP appliances in a SPAN configuration allowing NetWolves to monitor all user/device traffic.

Traffic Trending **-** answers the question, "What is going on in my network?" Using the same technology as mentioned in the "User Behavior" section, NetWolves has the ability to aggregate and classify all the traffic which traverses costly WAN circuits. NetWolves centers its attention on measuring the quantities of each traffic type in order to improve capacity planning.

A network flow can be defined in many ways. NetWolves defines a flow as a unidirectional sequence of packets that all share the following 7 values:

1. Ingress interface (SNMP ifIndex)
2. Source IP address
3. Destination IP address
4. IP protocol
5. Source port for UDP or TCP, 0 for other protocols
6. Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
7. IP Type of Service

Using the WolfPac Platinum deployed at each location, NetWolves aggregates and stores all NetFlow data within the SRM2-S Monitoring Environment for one (1) year.

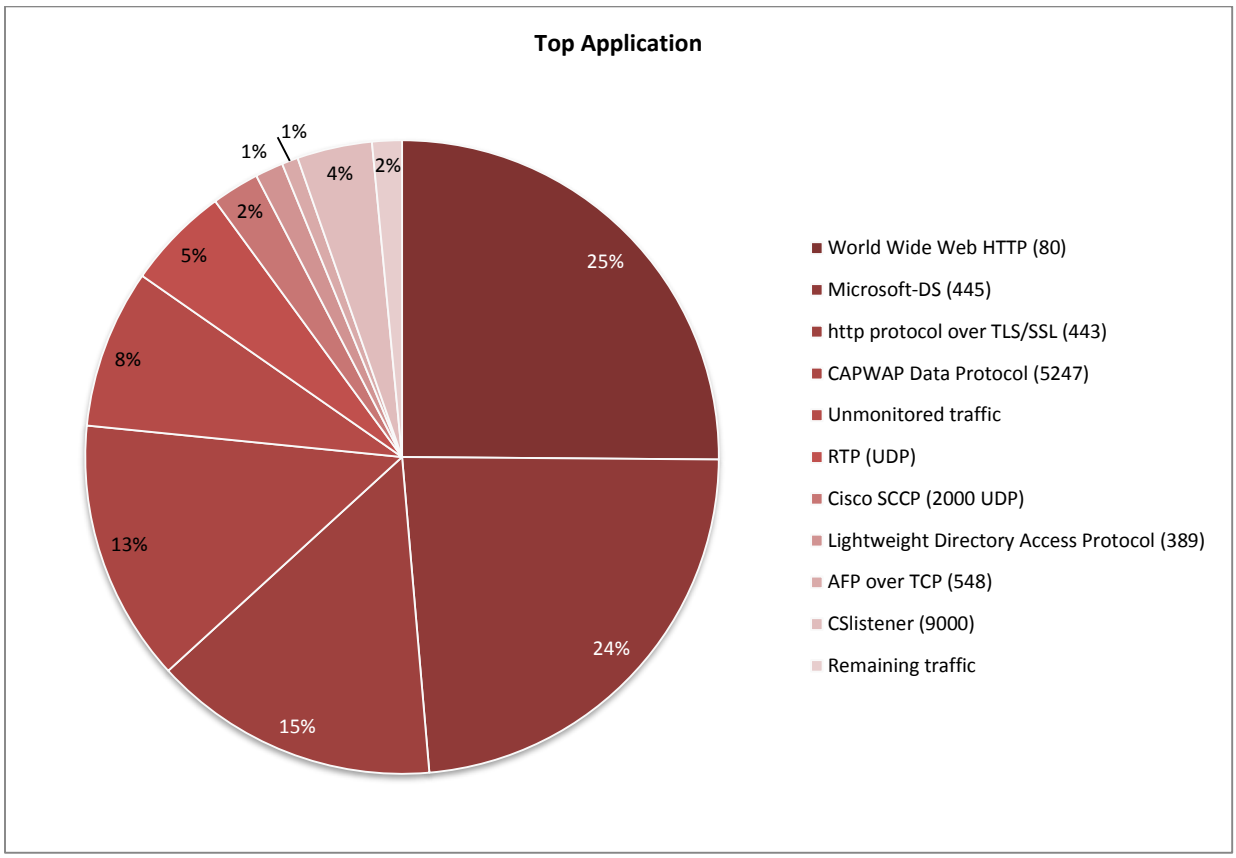
This data is also available through the NetWolves SRM^2-S monitoring dashboard accessible at: http://mno.netwolves.com.

(See Exhibit D for Details)

Top Applications

Network applications refer to applications that utilize the internet or other network hardware infrastructure to perform useful functions. Network software is a general phrase for software that is designed to help set up, manage, and/or monitor computer networks.

- All applications look related to normal day to day business.
- Unmonitored traffic may be identified with the assistance of Customer X.
    - The NetWolves SRM2-S Monitoring Environment records traffic with undefined TCP/UDP ports as Unmonitored. If requested, NetWolves will supply a list of all port numbers observed but must be identified by Customer X.



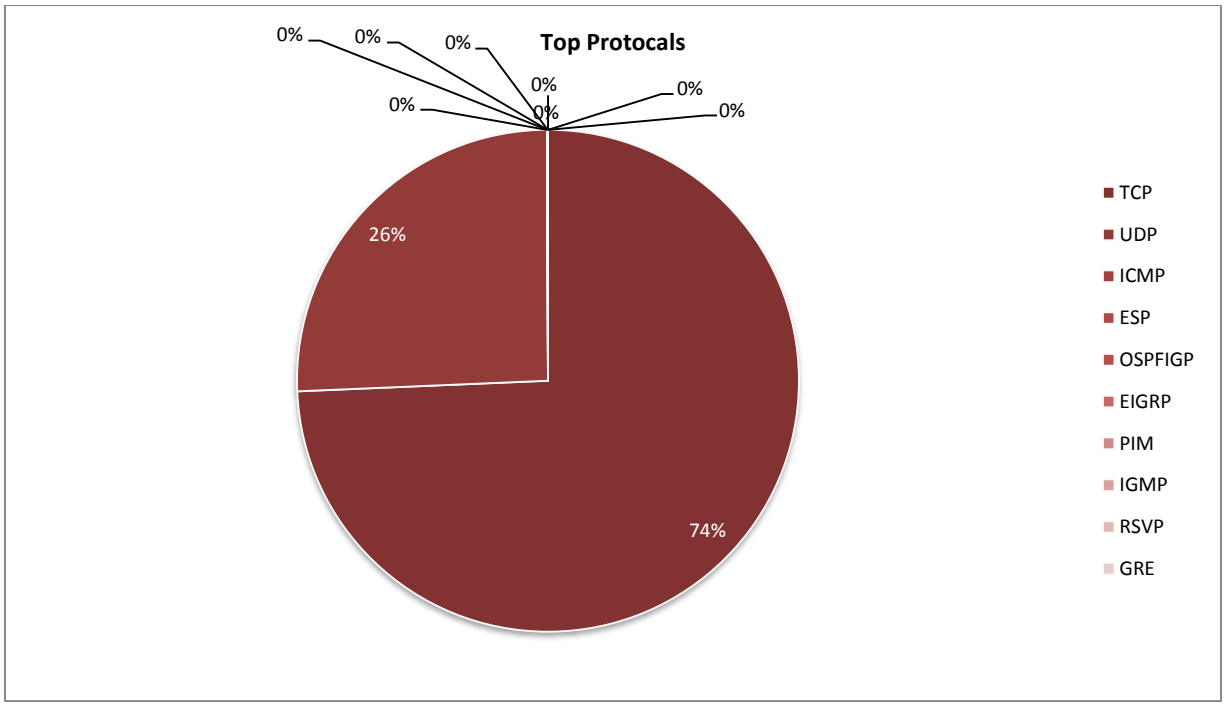
APPLICATION	Percentage	Ingress Traffic in Tbytes
World Wide Web HTTP (80)	25.97%	74.4
Microsoft-DS (445)	24.36%	69.6
http protocol over TLS/SSL (443)	15.07%	43.2
CAPWAP Data Protocol (5247)	14.07%	39.6
Unmonitored traffic	8.41%	24
RTP (UDP)	5.28%	15.6
Cisco SCCP (2000 UDP)	2.52%	7.2048
Lightweight Directory Access Protocol (389)	1.48%	4.2348
AFP over TCP (548)	0.86%	2.4564
CSlistener (9000)	0.40%	11.34
Remaining traffic	1.58%	4.4976

Top Protocol

TCP and UDP protocols account for **100%** of traffic. **TCP (74%)** is the Transmission Control Protocol and is one of the core protocols of the Internet Protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public internet. It resides at the transport layer. Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another. HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, Telnet and a variety of other protocols are typically encapsulated in TCP.

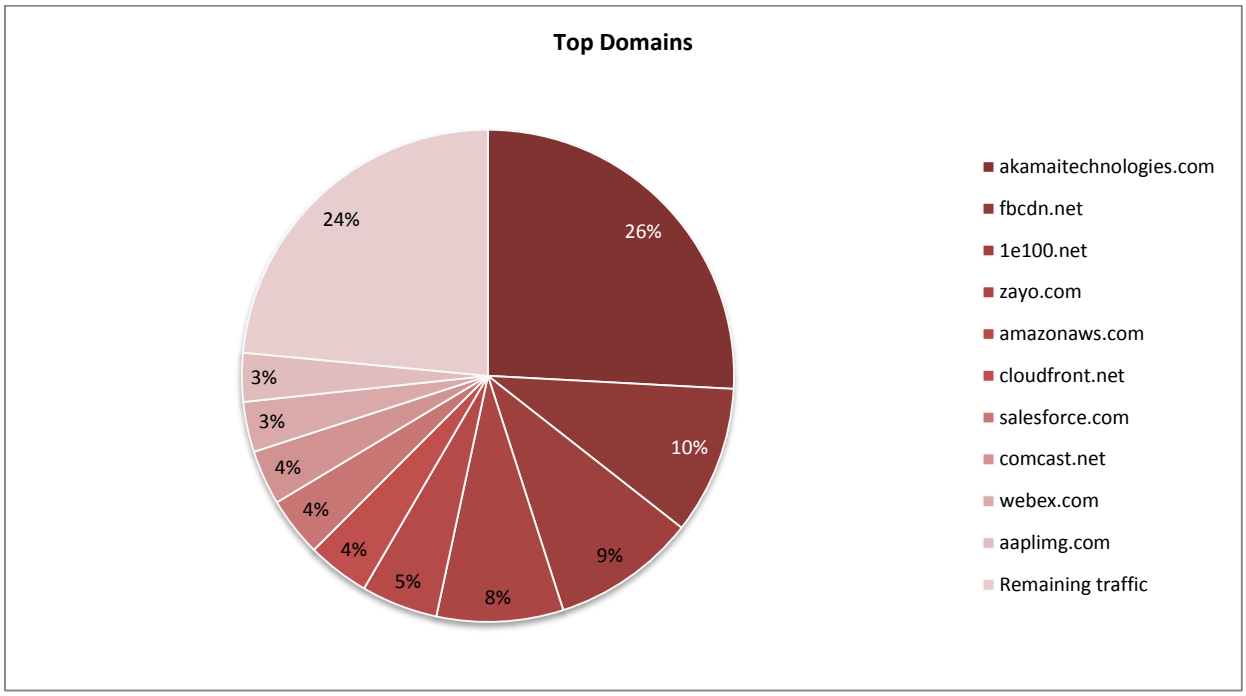
UDP (26%) uses a simple transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol to the user's program. As this is normally IP over unreliable media, there is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

As with all previous quarters, the TCP and UDP protocols are the most widely observed and expected.



PROTOCOL	Percentage	Ingress Traffic in Gbytes
TCP	74.23%	212400
UDP	25.71%	73200
ICMP	0.02%	50.4
ESP	0.01%	39.6
OSPFIGP	0.01%	34.8
EIGRP	0.01%	34.8
PIM	0%	7.896
IGMP	0%	2.4612
RSVP	0%	0.564
GRE	0%	0.045828

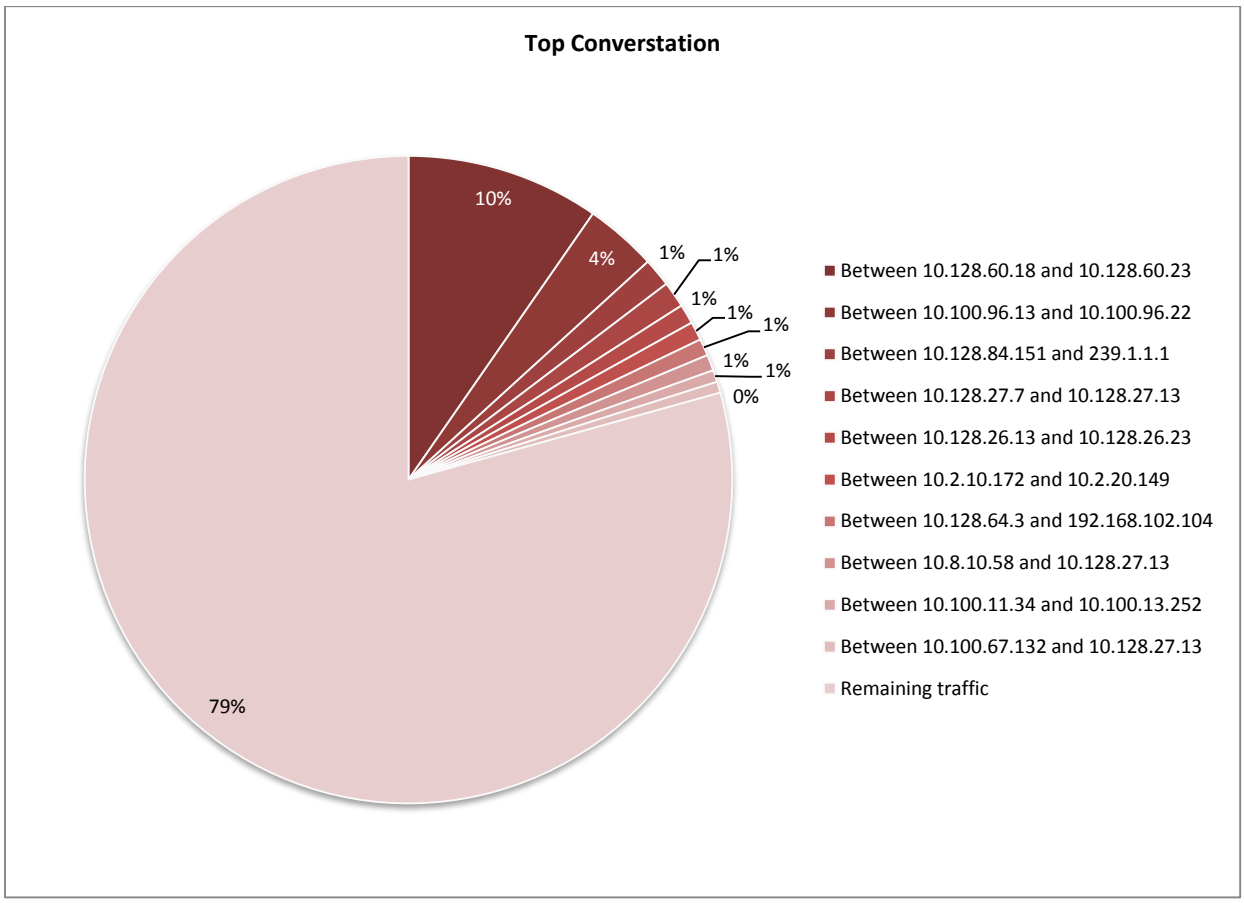
Top Domains



DOMAIN	Percentage	Ingress Traffic in Gbytes
akamaitechnologies.com	25.03%	13200
fbcdn.net	9.71%	4975.2
1e100.net	9.43%	4832.4
zayo.com	8.29%	4248
amazonaws.com	5.01%	2570.4
cloudfront.net	4.09%	2094
salesforce.com	3.89%	1995.6
comcast.net	3.59%	1838.4
webex.com	3.29%	1683.6
aaplimg.com	3.19%	1635.6
Remaining traffic	24.49%	12000

As with the last several quarters, Akami Technologies is once again the most visited domain along with Google, Facebook, SalesForce, Apple, ColudFrond, and One Drive.

Top Conversations



CONVERSATION	Percentage	Ingress Traffic in Tbytes
Between 10.128.60.18 and 10.128.60.23	9.61%	27.6
Between 10.100.96.13 and 10.100.96.22	3.60%	10.2744
Between 10.128.84.151 and 239.1.1.1	1.42%	4.0572
Between 10.128.27.7 and 10.128.27.13	1.30%	3.72
Between 10.128.26.13 and 10.128.26.23	0.98%	2.802
Between 10.2.10.172 and 10.2.20.149	0.93%	2.6556
Between 10.128.64.3 and 192.168.102.104	0.85%	2.418
Between 10.8.10.58 and 10.128.27.13	0.80%	2.2788
Between 10.100.11.34 and 10.100.13.252	0.60%	1.71
Between 10.100.67.132 and 10.128.27.13	0.56%	1.5912
Remaining traffic	79.36%	226.8

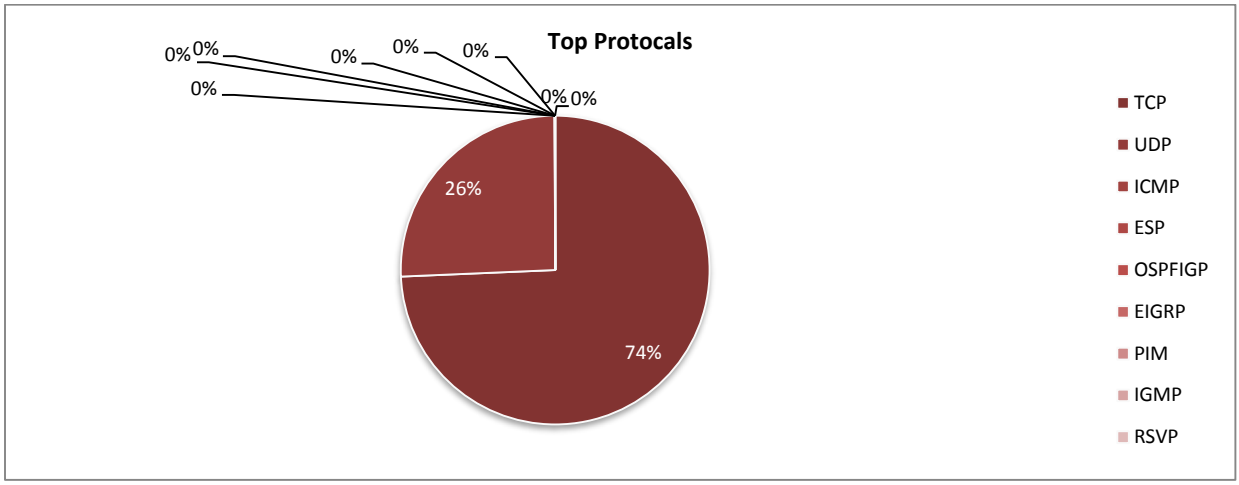
All traffic observed and recorded at top conversations for Q2 listed above have been analyzed and identified as legitimate business traffic.

Note: All traffic listed above is intranet based only.

Top Types of Service

The Type of Service field is present in IP Header and it was originally defined in RFC 791. The Type of Service octet consists of three fields. The last 3 bits (7, 6, and 5) are for the first field, labeled “Precedence”, intended to denote the importance or priority of the datagram. The second field, labeled “TOS”, denotes how the network should make tradeoffs between throughput, delay, reliability, and cost. The first field, labeled “MBZ” (for “must be zero”) above, is currently unused. The originator of a datagram sets this field to zero (unless participating in an Internet Protocol experiment which makes use of that bit). Routers and recipients of datagrams ignore the value of this field. This field is copied on fragmentation.

- All type of service match, including EF and AF41, proving the QOS is operating as expected.
- Unlike Top Applications, NetWolves is unable to further define Unknown Traffic within Types of Service.



PROTOCOL	Percentage	Ingress Traffic in Gbytes
TCP	74.23%	212400
UDP	25.71%	73200
ICMP	0.02%	50.4
ESP	0.01%	39.6
OSPFIGP	0.01%	34.8
EIGRP	0.01%	34.8
PIM	0%	7.896
IGMP	0%	2.4612
RSVP	0%	0.564
GRE	0%	0.045828

DSCP Name	DS Field Value (Dec)	IP Precedence (Description)
CS0	0	0 : Best Effort
CS1,AF11-13	8,10,12,14	1 :Priority
CS2,AF21-23	16,18,20,22	2 :Immediate
CS3,AF31-33	24,26,28,30	3 :Flash - mainly used for voice signaling
CS4,AF41-43	32,34,36,38	4 :Flash Override
CS5,EF	40,46	5 :Critical - mainly used for voice RTP
CS6	48	6 :Internet
CS7	56	7 :Network

NetWolves Managed Service

As a Platinum Managed Services subscriber, NetWolves provided Customer X Company Network Monitoring and Management, Project Management, and Executive Management during the Q2 2014.

Management:

RMAC (Reviews, Moves, Adds & Changes)

Definition: An RMAC is any work that will need to be completed which requires less than 8 hours designing and implementing by NetWolves SA/SD teams for an existing customer. RMAC's do not require any type of project management and are not additional billable items but are simply included as part of NetWolves managed services.

Total RMAC Tickets	3

RMAC Details	Ticket Opened	Ticket Type	Ticket State
Location X – enable Port 35 on Switch 7	4/6/15 2:48 PM	RMAC	Closed
Location X – Nursing Campus – schedule hot cut for BGP Timer Change	5/6/15 4:03 PM	RMAC	Pending
Customer X Data Center Data Center – inbound load sharing	6/29/15 2:49 PM	RMAC	Closed

(See Exhibit F for Details)

ECP (Existing Client Projects)

Definition: An ECP is any work that will need to be completed which requires more than 8 hours designing and implementing by NetWolves SA/SD teams for an existing customer. ECP's have a dedicated project manager, lead engineer, and Account manager participation. All ECP will require a signed SoW and design document by the customer.

Total ECP's	0

ECP Details	Status
Design a lab test for Performance Routing (PfR)	In process

(See Exhibit E for Details)

CPR (Critical Problem Review)

Definition: A service provided to MNO customers, which 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 SA teams to produce a CPR is defined as a critical production outage affecting multiple customer sites for durations of 2 hours or more or upon customer request.

Total CPR	0

(See Exhibit G for Details)

IM (Incident Management)

Definition: The processes and procedures created to identify, analyze and correct current and potential customer affecting issues to restore normal customer functionality and minimize customer downtime. Incident tickets are created to troubleshoot and track customer affecting outages or issues from inception to resolution. These tickets are the primary method of communication to our customers regarding the status of their outage or issue.

Of the 100 Tickets opened this quarter, 89 are classified as Incident. This is an increase of 34 incident tickets from the previous quarter. There were a total of 92 tickets opened last quarter, so there was an increase in total tickets as well as incidents tickets.

NetWolves has three (3) levels of severity when dealing with customer issues:

NetWolves has three (3) levels of severity when dealing with customer issues:

Total Incident Tickets

Total Incident Incidents	89

Urgent – Site is down; no connectivity, failover was unsuccessful or NetWolves declares an emergency. However, for Customer X Company, NetWolves considers any circuit or hardware incident to be Urgent.

Total Urgent Incidents	29

High – site is functioning in a degraded state or has failed to back up circuit and business has been minimally impacted.

Total High Incidents	45

Moderate – site is functioning in a degraded state but still operational (i.e. slowness/packet loss/circuit bounce and restored in under 2 minutes), or operating with one circuit in a bond inoperable (i.e., bonded T1, bonded broadband)

Total Moderate Incidents	5

- 10 tickets were created with no status.

Most Impactful Incidents

Location	Ocalla II
The primary MPLS circuit began to alarm at 3:45pm on 6/23 and restored at 7:45am 6/24. The facility provider reported the circuit bouncing every few minutes are requested the have the LAN cable tested or reseated. Once the cable was reseated, the alert cleared and traffic restored. During the duration of his outage, traffic routed across the secondary circuit.	

Location	Morehead
The primary MPLS Ethernet circuit went offline at 04/13/15 around 2:24 PM EST and restored at 04/13/15 at 2:54 PM EST. The facility provider verified that the reason of outage was due to a higher level central office issue.	

Location	Fargo
This location experienced multiple power outages totaling 240 minutes. One outage was due to UPS replacements on-site.	

Location	Rockford
This location experienced multiple power outages totaling 240 minutes. One outage was due to UPS replacements on-site.	

(See Exhibit H for Details)

NetWolves Managed Security Service

Managed Security Services Summary
MSS concentrates on providing a unique and best in class service offering, focused on securing and monitoring the client IT infrastructure from any intrusion or attack. NetWolves Network Services provides Customer X with a customized version of MSS to best meet the customer's needs.

Ticket Type	Total
Service Critical Incident & Ticket Details	11
Events	182

Perimeter Services:
The NetWolves architecture for MSS concentrates around functionality borders and perimeter points. These are most commonly where one security requirement touches another (i.e. where Internet access connects to a data center network). All systems that are both physically and logically connected as well as have the same security requirements represent a Security Zone. When one Security Zone requires resources from another, NetWolves will implement and manage a security appliance for policy enforcement, monitoring and event reporting. The logical point where these appliances will be inserted is known as a perimeter.

Aggregated URL filtering: URL filtering (also known as content filtering) is a service designed to restrict or control the content a user is authorized to access that is delivered over the Internet. Aggregated URL filtering is defined by NetWolves as a common policy for all users, which access the Internet on a per client basis. Specific users cannot have customizable permissions or reporting options, rather a global set of restrictions and permissions are deployed on a per client basis. Our current solution is based upon a Cisco Systems product known as Cisco Web Security (CWS). This is a "cloud" based product, which utilizes the IOS on the routers. The CWS service forwards web traffic to assigned proxies in CWS data centers, which scan it for malware and policy enforcement. Our MSS CPE, which must be an Integrated Services Router - Generation 2 (ISR-G2), will directly connect to the CWS service. CWS is priced and scaled with the number of users employing the service. This service will be completely managed by NetWolves' Operations and is transparent to the customer.

User Based URL Filtering: User based filtering allows for more granular policies and controls than the aggregated filtering. By utilizing next generation firewall

Perimeter based anti-virus & anti-spyware: Detects and blocks viruses, spyware phone home, spyware download, botnet, worms and Trojans when in-motion and attempting to traverse through the NGFW. By default, the security appliance inspects all of the listed protocol decoders for viruses, generates alerts for Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP), and Post Office Protocol Version 3 (POP3), and takes the default action for other applications (alert or deny), depending on the type of virus detected. Customized profiles can be used to minimize antivirus inspection for traffic between security zones.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): is a function of a security appliance that monitors our customer's networks for malicious activities and policy violations. Additionally, the appliance produces reports to our management systems. Intrusion detection and prevention are primarily focused on identifying possible incidents, logging information about them, reporting attempts, identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. NetWolves has taken a unique approach to the way this product is delivered. IBM and Palo Alto Networks (PAN) have partnered with NetWolves to provide this robust and efficient solution.

Additionally, NetWolves utilizes the IBM SOC (Secure Operations Center) for Syslog parsing and intrusion alerting. The PAN platform exports Syslog data to an aggregation server and forward the data to all IBM SOC's for alert detection. Utilizing this process, 15 security incidents have been caught and remediated to date. The following section details the information gathered and sent to the SOC for analysis.

Quarterly Statistics SOC:

Security Incidents: Events with verifiable malicious intent or that suggest an element of unusual risk as detected by the IBM SOC Managed Security Solution.

All Critical Incidents for Q3 are related to ANGLER Exploit Kits. These kits are hacking tool that are produced to search for Java and Flash Player vulnerabilities on the attacked PC and use them with the aim to distribute malware infections. Angler Exploit Kit commonly checks to see if the PC it is proliferating to has Java or Flash

Service Critical Incident & Ticket Details

Alert Date	Ticket Number	Description	SOC Actions	Recommended Actions
9/10/2015 13:34	702949015	ANGLER Exploit Kit Detection(37744)	Checked special instructions and found nothing relevant to this specific alert - Checked the acceptable traffic list - Investigated the logs	Please investigate the target IP host immediately - If the host contains sensitive information, take steps to preserve the machine for forensic investigation.
8/20/2015 16:21	702903930	NGLER Exploit Kit Detection(37744)	checked special instructions and found nothing relevant to this specific alert - Checked the acceptable traffic list - Investigated the logs - Source IP address is listed on our Global Attackers list but not blacklisted	Please investigate the target IP host immediately - If the host contains sensitive information, take steps to preserve the machine for forensic investigation
7/15/2015 16:10	702838036	ANGLER Exploit Kit Detection(37796)	Check acceptable traffic, special instructions and research tab. Check raw data and analyze the information on it. Verify the IP addresses. Notify the customer	Please verify the legitimacy of this traffic. Check your system has not been compromised and up-to-date with latest AV, Signatures and patches.
7/14/2015 18:56	702836513	ANGLER Exploit Kit Detection(37744)	Checked the Source and destination IPs and determined this can be handled as a suspicious activity on the network Source IP Information IP Address Information Analysis Date 15 seconds ago Blacklist Status POSSIBLY SAFE 0/40 IP Address 185.48.58.52 (Websites Lookup) Reverse DNS localhost1.ru ASN AS62088 ASN Owner Sinarohost LTD ISP Unknown Continent Europe Country Code Flag (NL) Netherlands Latitude / Longitude 52.3667 / 4.9 City Unknown Region Unknown	It is recommended to check the source and destination IPs to determine if there was no data corruption or unauthorized access. It is also recommended to block this source if it is not a listed acceptable traffic source. Would you like us to take action in regard to this traffic? A). Block the signature on your managed device. B). Filter this traffic on your managed device. C). Filter this traffic on our console. The device will still log the traffic, but will not be reported or escalated. We can filter by IP address source(s), IP destination(s), signature or any combination of the three. Our recommendation is to block this signature on your managed device. You would no longer see escalations for this traffic.
07/15/15 16:10	702838036	ANGLER Exploit Kit Detection(37796)	Check acceptable traffic, special instructions and research tab. Check raw data and analyze the information on it. Verify the IP addresses. Notify the custome	Please verify the legitimacy of this traffic. Check your system has not been compromised and up-to-date with latest AV, Signatures and patches.

7/16/2015 18:51	702840670	ANGLER Exploit Kit Detection(37796)	Checked special instructions and found nothing relevant to this specific alert Checked the acceptable traffic list Checked the customer environment list and found nothing relevant to the source/destination IP address Checked the source/destination IP address lookup for any reported blacklist information: IP Address Information Analysis Date 3 seconds ago Blacklist Status POSSIBLY SAFE 0/40 IP Address 5.79.85.242 (Websites Lookup) Reverse DNS lw363.ua-hosting.company ASN AS60781 ASN Owner LeaseWeb B.V. ISP LeaseWeb B.V. Continent Europe Country Code Flag (NL) Netherlands Latitude / Longitude 52.35 / 4.9167 City Amsterdam Region Noord-Holland Escalated to customer	Please check if the activity is authorized, otherwise proceed checking for any signs of compromise within your network. In case you don't recognize the source host, you can also proceed taking the necessary precautions by blocking it within your perimeter firewall. Also check if you are running an up-to-date AV and also check if the latest patches are applied to your system/servers/devices in general.
7/13/2015 11:53	702834130	ANGLER Exploit Kit Detection(37744)	Checked Special Instructions for information related to the event. Notified customer via email concerning the event. Checked for Global Attackers Investigated previous escalations for additional information concerning the event. Researched source IP for additional events in the previous 2 hours. Researched destination IP for return traffic to the source in the previous 2 hours. Examined event IDS/IPS logs, check raw data for additional data to include in the alert. Checked for additional logs in Correlated Log Details.	Review traffic and determine if this was authorized activity.
7/17/2015 12:49	702841858	ANGLER Exploit Kit Detection(37744)	Examined event IDS/IPS logs, check raw data for additional data to include in the alert. Checked for additional logs in Correlated Log Details. Checked Special Instructions Global attacker is verified against involved IPs Customer was contacted via email about these events.	The source ip is currently blacklisted in IP Void.Consider blocking the IP if found unauthorized for this action. Apply patches/upgrades to the target machine as per vendor recommendation. Use great caution when opening attachments. Configure antivirus software to automatically scan all email and instant-message attachments. Make sure email programs do not automatically open attachments or automatically render graphics,and ensure that the preview pane is turned off. Never open unsolicited emails, or unexpected attachments—even from known people. Beware of spam-based phishing schemes. Don’t click on links in emails or instant messages.

				Use a browser plug-in to block the execution of scripts and iframes
7/24/2015 15:57	702855065	ANGLER Exploit Kit Detection(37744)	Checked special instructions and found nothing relevant to this specific alert - Checked the acceptable traffic list - Investigated the logs	Please investigate the target IP host immediately - If the host contains sensitive information, take steps to preserve the machine for forensic investigation.
7/10/2015 16:26	702830874	ANGLER Exploit Kit Detection(37744)	Examined IDS and Correlated log details, and Research Tab. Global Attacker identified. Checked Special Instructions Customer was contacted via e-mail about these events.	Please verify the legitimacy of this traffic. Check that your system has not been compromised and is up-to-date with latest anti-malware software, signatures and patches. Investigate the targeted machines for signs of unauthorized access/changes and if needed block the offending source. Please, also ensure that comprehensive software update policies are in place.
7/1/2015 18:05	702816469	ANGLER Exploit Kit Detection(37744)	Checked special instructions and found nothing relevant to this specific alert - Checked the acceptable traffic list - Investigated the logs - Source IP address is listed on our Global Attackers list and it's not blacklisted at this moment.	Please investigate the target IP host immediately - If the host contains sensitive information, take steps to preserve the machine for forensic investigation.

(For details including the RAW Event, see exhibit M)

Alert Activity

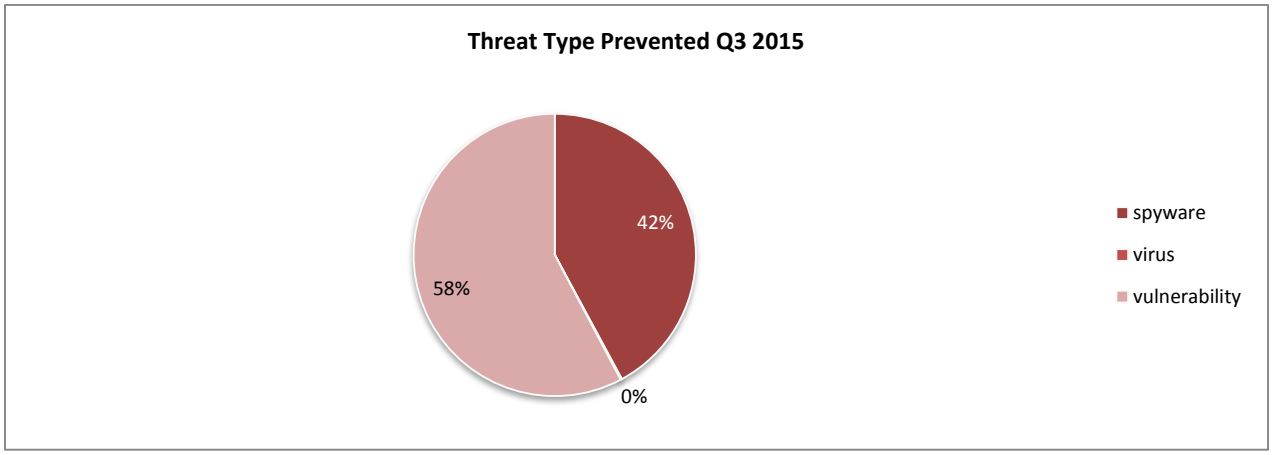
Issue	Count
FWIncreaseConnectionsAllowed	70
FWIncreaseProtocolAllowed	48
ScanningToolsUniqSRCDetectionRule	44
FWNewEntryInTopAllowedConnections	33
FWNewEntryInTopDeniedConnections	7
FWNewEntryInTopAllowedProtocol	4
XSS_GeneralAttack	3
FWNewEntryInTopDeniedProtocol	2
FWIncreaseProtocolDenied	1
FWIncreaseTargettedIp	1
FWNewEntryInTopDeniedTraffic	1

FWNewEntryInTopTargettedIp	1
FWNewEntryInTopTrafficSummaryAll	1
FWTotalDeniedTrafficDecrease	1
Malicious_Website	1
Total	**218**

Quarterly Firewall Threat Prevention Statistics:

The below section details statistics collected by the Palo A lot firewall utilized for Aggregated URL filtering, User Based URL Filtering, Perimeter based anti-virus & anti-spyware, and IDS/IPS (Intrusion Detection System/Intrusion Prevention System).

See exhibit L for further details



Threat Type Prevented	Total
Spyware	2,229
Virus	8
Vulnerability	3,055
Total	5,292

Top 20 Threats:

Threat/Content Name	ID	Threat/Content Type	Count
Microsoft Windows win.ini access attempt	30851	vulnerability	620
Generic HTTP Cross Site Scripting Attempt	31476	vulnerability	426
RFC2397 Data URL Scheme Usage Detected	30419	vulnerability	335
Suspicious DNS Query (None:obygqj.com)	4099496	spyware	292
Suspicious DNS Query (None:ufudiku.bexonpx.com)	4063075	spyware	268
Bash Remote Code Execution Vulnerability	36729	vulnerability	234
Cisco Catalyst Remote Arbitrary Command Execution Vulnerability	30920	vulnerability	210
SSH User Authentication Brute-force Attempt	40015	vulnerability	204
kovter.Gen Command And Control Traffic	14737	spyware	200
HTTP /etc/passwd Access Attempt	30852	vulnerability	158
Apache Struts2 IncludeParams Remote Code Execution Vulnerability	36231	vulnerability	140
Suspicious DNS Query (None:overuxona.bexonpx.com)	4033217	spyware	138
Suspicious DNS Query (None:anyljxqbew.bexonpx.com)	4033213	spyware	137
Suspicious DNS Query (None:obavyjyfyt.bexonpx.com)	4033227	spyware	120
Suspicious DNS Query (None:itabobajymy.bexonpx.com)	4033229	spyware	111

Suspicious DNS Query (None:amcsmy.com)	4012574	spyware	89
Suspicious.Gen Command And Control Traffic	14700	spyware	84
Microsoft Windows SMBv2 Remote Code Execution Vulnerability	32541	vulnerability	80
Suspicious DNS Query (None:nqlsxsviv.org)	4012573	spyware	79
MS-RDP Brute-force Attempt	40021	vulnerability	74

Prevented Virus Review

Name:	TrojanDownloader/Win32.upatre.bipx
Description:	This is a Trojan detection. Unlike viruses, trojans do not self-replicate. They are spread manually, often under the premise that they are beneficial or wanted. The most common installation methods involve system or security exploitation, and unsuspecting users manually executing unknown programs. Distribution channels include email, malicious or hacked web pages, Internet Relay Chat (IRC), peer-to-peer networks, etc.
Risk Assessment:	Low
Date Discovered:	1/20/2014
Date Added:	10/20/2013
Origin:	Unknown
Length:	0
Type:	Trojan
Subtype:	Email Self-extracting archiv
DAT Required:	7324
System Changes:	"Generic.qe" is a generic detection for a Trojan. This is a message file with a Trojan archived in it which will get detected as RDN/Generic Downloader.x!jl. The below are Characteristics of the archived Trojan. Upon execution, Trojan connects to the following IP Addresse through remote port https: 67.228.[Removed].218 23.11.[Removed]5.40 121.6.[Removed].119 61.32.[Removed].131 172.245.[Removed].122 60.244.[Removed].6 207.251.[Removed].31 62.49.[Removed].189 81.149.[Removed].130 77.242.[Removed].250 107.[Removed]239.26 84.59.[Removed]9.23 27.[Removed].110.77 132.[Removed].151.194 81.[Removed].43.98 121.[Removed].214.103 76.[Removed].224.199 125.[Removed].56.233 139.[Removed].159.141 86.[Removed].15.3 176.[Removed].92.169 81.[Removed].210.54 81.[Removed].228.176 178.[Removed].201.245 111.[Removed].140.240 67.[Removed].17.157 81.[Removed].233.196 88.[Removed].94.219 95.[Removed].2.108 213.[Removed].204.220 59.[Removed].205.36 121.[Removed].137.227 73.[Removed].33.45 203.[Removed].76.86 126.[Removed].45.61 84.[Removed].138.122 86.[Removed].174.251 109.[Removed]1.115.21 175.2[Removed]12.2 58.[Removed].45.152 31.[Removed].66.129 217.81.10.20 80.15.[Removed].62 81.[Removed].198.69 On execution, it drops the below files. %AppData%\Teamp\ectuus.exe %Temp%\sysupdate.exe

	%Temp%\chong.exe %UserProfile%\Local Settings\Temporary Internet Files\Content.IE5\L1QH00M8\wav[1].exe The following are the registry key have been added to the system. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Internet Explorer\Toolbar\Explorer HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy The following registry key value have been added to the system. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\DisableNotifications: 0x00000000 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\WINDOWS\explorer.exe: "C:\WINDOWS\explorer.exe:*:Enabled:Windows Explorer" HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\3471:UDP: "3471:UDP:*:Enabled:UDP 3471" HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\1221:TCP: "1221:TCP:*:Enabled:TCP 1221" HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\DisableNotifications: 0x00000000 HKEY_USER\S-1-5-21-[Varies]\Identities\Identity Login: 0x00098053 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser\{01E04581-4EEE-11D0-BFE9-00AA005B4383}: 81 45 E0 01 EE 4E D0 11 BF E9 00 AA 00 5B 43 83 10 00 00 00 00 00 00 00 01 E0 32 F4 01 00 00 00 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Internet Explorer\Toolbar\Explorer\ITBarLayout: [Binary Value] HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\WAB\WAB4\FirstRun: 0x00000001 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\View: [Binary Value] HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\FindFlags: 0x0000000E HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\LastKey: "My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Windows\CurrentVersion\Run\Ectuus: ""%AppData%\Teamp\ectuus.exe"" The above mentioned registry ensures that, the Trojan registers run entry with the compromised system and execute itself upon every boot. HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{7BD29E01-76C1-11CF-9DD0-00A0C9034933} {000214E6-0000-0000-C000-000000000046} 0x401: 01 00 00 00 31 00 38 00 EC 64 3D 78 13 1C CF 01 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\2f3h1f1d: B3 EC 84 6B 91 0C 70 A8 E4 15 10 80 89 06 E2 A6 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\2a7i5ba7: 0x6BB5ECD0 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\1aadgc8b: 0E E1 B5 6B 01 08 3B A8 C9 15 63 80 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\2ihh9482: [Binary Value] HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\24di3eca: [Binary Value] HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\16j07839: [Binary Value] HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\2d6gaidf: [Binary Value] HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\2h1ide31: A9 6A 52 39 HKEY_USER\S-1-5-21-[Varies]\Software\Microsoft\Joifwivipy\1a7051d2: [Binary Value]

Name:	TrojanDownloader/Win32.upatre.bipx
Description:	TrojanDownloader:Win32/Upatre is defined as a malicious trojan infection with great risks. The virus has the capacity to malfunction the system settings randomly. And TrojanDownloader:Win32/Upatre is able to execute malicious processes without asking permission. Due to this TrojanDownloader:Win32/Upatre virus, other malware actions can activate themselves to damage the system. Usually TrojanDownloader:Win32/Upatre comes from malicious malware download process. It sneaks into the system without asking permission. Users did not realize the TrojanDownloader:Win32/Upatre infection until antivirus programs alert them. However, TrojanDownloader:Win32/Upatre is very tricky, it can hide deeply in the system and root into other important files. TrojanDownloader:Win32/Upatre is very good at stealing the personal information. When it infiltrates into the system, if there are information concerning about banking data, accounts passwords, credit card password and also other sensitive personal info., users are under high risks to privacy leakage. Besides, this TrojanDownloader:Win32/Upatre can accommodate details of all of your drives on the targeted computers.
Risk Assessment:	Low
Date Discovered:	2/19/2015
Date Added:	2/20/2015
Origin:	Unknown
Length:	1013760
Type:	Virus
Subtype:	Win32
DAT Required:	N/A
System Changes:	Some path values have been replaced with environment variables as the exact location may vary with different configurations. e.g. %WINDIR% = \WINDOWS (Windows 9x/ME/XP/Vista/7), \WINNT (Windows NT/2000) %PROGRAMFILES% = \Program Files The following files have been added to the system: %TEMP%\LMablscn.exe C:\Documents and Settings\LocalService\OoAQEsEg\aawgQUIg %USERPROFILE%\OoAQEsEg\aawgQUIg %ALLUSERSPROFILE%\swkAlkoo\rKccsAoM %ALLUSERSPROFILE%\lwQg.txt %ALLUSERSPROFILE%\xkkkEYUo\CcEYQQAE.exe %ALLUSERSPROFILE%\swkAlkoo\rKccsAoM.exe %USERPROFILE%\OoAQEsEg\aawgQUIg.exe The following files were temporarily written to disk then later removed: %TEMP%\TiQgAMQA.bat The following registry elements have been changed: HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\ADVANCED\HIDDEN = 2 HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\ADVANCED\HIDEFILEEXT = 1 HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\AAWGQUIG.EXE = %USERPROFILE%\OoAQEsEg\aawgQUIg.exe HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\USERINIT = %WINDIR%\SYSTEM32\userinit.exe,%ALLUSERSPROFILE%\swkAlkoo\rKccsAoM.exe, HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM\ENABLELUA = 0 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\RKCCSAOM.EXE = %ALLUSERSPROFILE%\swkAlkoo\rKccsAoM.exe The applications attempted the following network connection(s): 216.58.216.**:80 %WINDIR% = \WINDOWS (Windows 9x/ME/XP/Vista/7), \WINNT (Windows NT/2000) %PROGRAMFILES% = \Program Files

Name:	Virus/Win32.virut.btwjy
Description:	W32/Virut.b is a file infecting virus. It tries to infect executable files that are accessed once the virus is active. W32/Virut.b opens up a backdoor on the infected machine and contacts an IRC server to receive bot commands.
Risk Assessment:	Low
Date Discovered:	6/12/2006
Date Added:	6/12/2006
Origin:	N/A
Length:	N/A
Type:	Virus
Subtype:	Win32
DAT Required:	4782
System Changes:	W32/Virut.b is a file infecting virus. On execution it copies itself in %SYSTEMDIR%\dllcache as msiupdate32.exe. It then tries to infect accessed executables. It may also infect %SYSTEMDIR%\cmd.exe. Registers itself as a service using the following registry entry: hkey_local_machine\system\currentcontrolset\services\microsoft update service objectname="LocalSystem" type="32" start="2" description="Microsoft update Service." displayname="Microsoft update Service" errorcontrol="0" imagepath=""%SYSTEMDIR%\dllcache\msiupdate32.exe"" W32/Virut.b opens up backdoor at random ports on the compromised machine. This virus tries to connect to IRC servers located at : dhl4.irc-sgo.org proxima.ircgalaxy.pl Following channel names may be used : ##teddy## ##td## ##kd## ##cd## ##proxy## ##sniff## ##test## Channel topics are accpeted as commands by the virus. The commands that the virus can receive include: Scan for vulnerable systems Download / execute remote files Start, stop the spread through IM Log keystrokes (primarily for stealing bank passwords) Open a command shell Format drive

Exhibits

Exhibit A: Device Availability

MPLS Availability (Sorted by Least Available)

Node	Average Availability
Customer X-appleton-MR-1-90302307	100.00%
Customer X-appleton-MR-2-90302307	100.00%
Customer X-aurora-MR-1-90302284	100.00%
Customer X-aurora-MR-2-90302284	100.00%
Customer X-bismarck-MR-1-90302285	100.00%
Customer X-bismarck-MR-2-90302285	100.00%
Customer X-blaine-MR-1-90302305	100.00%
Customer X-blaine-MR-2-90302305	100.00%
Customer X-brandon-MR-1-90302610	100.00%
Customer X-brandon-MR-2-90302610	100.00%
Customer X-brooklyn-MR-1-90302286	100.00%
Customer X-brooklyn-MR-2-90302286	100.00%
Customer X-deltak-MR-1-200008745	100.00%
Customer X-deltak-MR-2-200008745	100.00%
Customer X-eagan-MR-1-90302288	100.00%
Customer X-eagan-MR-2-90302288	100.00%
Customer X-fargo-MR-1-90302291	100.00%
Customer X-fargo-MR-2-90302291	100.00%
Customer X-fortmyer-MR-1-90302289	100.00%
Customer X-fortmyer-MR-2-90302289	100.00%
Customer X-greenbay-MR-1-90302290	100.00%
Customer X-greenbay-MR-2-90302290	100.00%
Customer X-lakeelmo-MR-1-90302293	100.00%
Customer X-lakeelmo-MR-2-90302293	100.00%
Customer X-landolak-MR-1-200000071	100.00%
Customer X-landolak-MR-2-200000071	100.00%
Customer X-Customer X Data Center-MR-1-200006001	100.00%
Customer X-Customer X Data Center-MR-2-200006001	100.00%
Customer X-maitland-MR-1-90302296	100.00%
Customer X-maitland-MR-2-90302296	100.00%
Customer X-mankato-MR-1-90302294	100.00%
Customer X-mankato-MR-2-90302294	100.00%
Customer X-mokena-MR-1-90302304	100.00%
Customer X-mokena-MR-2-90302304	100.00%
Customer X-moorhead-MR-1-90302295	100.00%
Customer X-moorhead-MR-2-90302295	100.00%
Customer X-newportr-MR-1-85556104	100.00%
Customer X-newportr-MR-2-85556104	100.00%

Internet Availability (Sorted by Least Available)

Node	Average Availability
Customer X-Aurora-IR-1-90302284	100.00%
Customer X-greenbay-IR-1-90302290	100.00%
Customer X-Customer X Data Center-IR-1-200006001	100.00%
Customer X-Customer X Data Center-IR-2-200006001	100.00%
Customer X-romeovil-IR-1-90302300	100.00%

Core Switch Availability

Node	Average Availability
Customer X-oakbrook-CS-1-90302309	99.97%
Customer X-twomarke-CS-1-85556374	100.00%
Customer X-bismarck-CS-1-90302285	100.00%
Customer X-maitland-CS-1-90302296	100.00%
Customer X-lakeelmo-CS-1-90302293	100.00%
Customer X-ocala1-CS-1-200003261	100.00%
Customer X-twinciti-CS-1-90302306	100.00%
Customer X-brandon-CS-1-90302610	100.00%
Customer X-eagan-CS-1-90302288	100.00%
Customer X-mokena-CS-1-90302304	100.00%
Customer X-landolak-CS-1-200000071	100.00%
Customer X-appleton-CS-1-90302307	100.00%
Customer X-mankato-CS-1-90302294	100.00%
Customer X-newportr-CS-1-85556104	100.00%
Customer X-overland-CS-1-200003610	100.00%
Customer X-blaine-CS-1-90302305	100.00%
Customer X-brooklyn-CS-1-90302286	100.00%
Customer X-moorhead-CS-1-90302295	100.00%
Customer X-ocala2-CS-1-90302308	100.00%
Customer X-romeovil-CS-1-90302300	100.00%
Customer X-wausau-CS-1-90302303	100.00%
Customer X-fargo-CS-1-90302291	100.00%
Customer X-fortmyer-CS-1-90302289	100.00%
Customer X-greenbay-CS-1-90302290	100.00%
Customer X-topeka-CS-1-200003611	100.00%

Switch Availability

Node	Average Availability
Customer X-fortmyer-SW-1-90302289	99.96%
Customer X-Customer X Data Center-SW-4-200006001	99.99%
Customer X-bismarck-SW-4-90302285	100.00%
Customer X-brooklyn-SW-11-90302286	100.00%
Customer X-brooklyn-SW-6-90302286	100.00%
Customer X-eagan-SW-5-90302288	100.00%
Customer X-Customer X Data Center-SW-3-200006001	100.00%
Customer X-moorhead-SW-4-90302295	100.00%
Customer X-twinciti-SW-4-90302306	100.00%
Customer X-twomarke-SW-1-85556374	100.00%
Customer X-eagan-SW-2-90302288	100.00%
Customer X-eagan-SW-7-90302288	100.00%
Customer X-fortmyer-SW-3-90302289	100.00%
Customer X-Customer X Data Center-SW-11-200006001	100.00%
Customer X-Customer X Data Center-SW-2-200006001	100.00%
Customer X-maitland-SW-3-90302296	100.00%
Customer X-oakbrook-SW-3-90302309	100.00%
Customer X-appleton-SW-2-90302307	100.00%
Customer X-bismarck-SW-11-90302285	100.00%
Customer X-Brooklyn-SW-8-90302286	100.00%
Customer X-eagan-SW-4-90302288	100.00%
Customer X-Customer X Data Center-SW-8-200006001	100.00%
Customer X-maitland-SW-1-90302296	100.00%
Customer X-mankato-SW-11-90302294	100.00%
Customer X-mankato-SW-6-90302294	100.00%
Customer X-oakbrook-SW-4-90302309	100.00%
Customer X-twinciti-SW-3-90302306	100.00%
Customer X-stcloud-SW-8-90302301	100.00%
Customer X-oakbrook-SW-9-90302309	100.00%
Customer X-rockford-SW-4-90302299	100.00%
Customer X-rockford-SW-7-90302299	100.00%
Customer X-brooklyn-SW-7-90302286	100.00%
Customer X-fargo-SW-4-90302291	100.00%
Customer X-maitland-SW-5-90302296	100.00%
Customer X-rockford-SW-2-90302299	100.00%
Customer X-fargo-SW-5-90302291	100.00%
Customer X-Customer X Data Center-SW-10-200006001	100.00%
Customer X-ocala1-SW-1-200003261	100.00%
Customer X-aurora-SW-2-90302284	100.00%

Exhibit B: Network Node Performance – CPU/Memory Utilization

Node	Average CPU Load	Average Percent Memory Used	Peak CPU Load
Customer X-greenbay-CS-1-90302290	38.00%	51.00%	49.00%
Customer X-romeovil-CS-1-90302300	38.00%	62.00%	42.00%
Customer X-wausau-CS-1-90302303	35.00%	55.00%	55.00%
Customer X-Customer X Data Center-SW-12-200006001	34.00%	13.00%	42.00%
Customer X-Customer X Data Center-SW-1-200006001	31.00%	13.00%	43.00%
Customer X-mankato-CS-1-90302294	31.00%	48.00%	42.00%
Customer X-fortmyer-CS-1-90302289	30.00%	50.00%	37.00%
Customer X-Customer X Data Center-SW-11-200006001	30.00%	13.00%	42.00%
Customer X-aurora-SW-1-90302284	29.00%	55.00%	33.00%
Customer X-blaine-CS-1-90302305	27.00%	50.00%	82.00%
Customer X-landolak-CS-1-200000071	26.00%	44.00%	34.00%
Customer X-mokena-CS-1-90302304	25.00%	49.00%	48.00%
Customer X-lakeelmo-CS-1-90302293	24.00%	45.00%	29.00%
Customer X-twinciti-WP-1-90302306	24.00%	14.00%	59.00%
Customer X-oakbrook-MR-1-90302309	23.00%	9.00%	68.00%
Customer X-twomarke-CS-1-85556374	22.00%	50.00%	30.00%
Customer X-maitland-WP-1-90302296	21.00%	16.00%	53.00%
Customer X-ocala1-CS-1-200003261	21.00%	29.00%	23.00%
Customer X-newportr-SW-1-85556104	19.00%	47.00%	21.00%
Customer X-oakbrook-WP-1-90302309	19.00%	13.00%	40.00%
Customer X-brandon-CS-1-90302610	18.00%	59.00%	22.00%
Customer X-ocala2-CS-1-90302308	18.00%	62.00%	23.00%
Customer X-rockford-VR-1-90302299	18.00%	66.00%	56.00%
Customer X-appleton-CS-1-90302307	17.00%	48.00%	22.00%
Customer X-Customer X Data Center-FW-2-200006001	17.00%	32.00%	37.00%
Customer X-maitland-MR-1-90302296	17.00%	9.00%	48.00%
Customer X-newportr-CS-1-85556104	17.00%	48.00%	21.00%
Customer X-bismarck-SW-11-90302285	16.00%	17.00%	24.00%
Customer X-fargo-SW-5-90302291	16.00%	28.00%	21.00%
Customer X-twinciti-MR-1-90302306	16.00%	9.00%	53.00%
Customer X-bismarck-CS-1-90302285	14.00%	19.00%	26.00%
Customer X-stcloud-SW-8-90302301	14.00%	62.00%	18.00%
Customer X-stcloud-SW-4-90302301	13.00%	20.00%	20.00%
Customer X-bismarck-SW-4-90302285	12.00%	28.00%	20.00%
Customer X-fortmyer-WP-1-90302289	12.00%	12.00%	25.00%
Customer X-ocala1-SW-1-200003261	12.00%	18.00%	18.00%
Customer X-stcloud-SW-3-90302301	12.00%	20.00%	20.00%
Customer X-stcloud-VR-1-90302301	12.00%	66.00%	32.00%
Customer X-twomarke-WP-1-85556374	12.00%	10.00%	32.00%
Customer X-fortmyer-SW-1-90302289	11.00%	18.00%	20.00%
Customer X-fortmyer-SW-2-90302289	11.00%	28.00%	23.00%

Exhibit C: Network Node Performance – Interface Utilization

Node	Interface	Recv Percent Util	Xmit Percent Util	Peak Receive bps	Peak Transmit bps
Customer X-appleton-VR-1-90302307	Serial0/1/0:16	0.00%	0.00%	0 bps	0 bps
Customer X-appleton-VR-1-90302307	Serial0/1/0:21	0.00%	0.00%	0 bps	0 bps
Customer X-aurora-VR-1-90302284	Serial0/0/0:11	0.00%	0.00%	0 bps	0 bps
Customer X-aurora-VR-1-90302284	Serial0/0/0:7	0.00%	0.00%	0 bps	0 bps
Customer X-brandon-VR-1-90302610	Serial0/0/0:1	0.00%	0.00%	0 bps	0 bps
Customer X-brandon-VR-1-90302610	Serial0/0/0:12	0.00%	0.00%	0 bps	0 bps
Customer X-brooklyn-VR-1-90302286	FastEthernet0/1	0.00%	0.15%	1559 bps	889 Kbps
Customer X-brooklyn-VR-1-90302286	Serial0/1/0:13	0.00%	0.00%	0 bps	0 bps
Customer X-brooklyn-VR-1-90302286	Serial0/1/0:18	0.00%	0.00%	0 bps	0 bps
Customer X-deltak-VR-1-200008745	Serial0/0/0:0	0.00%	0.00%	0 bps	0 bps
Customer X-deltak-VR-1-200008745	Serial0/0/0:10	0.00%	0.00%	0 bps	0 bps
Customer X-deltak-VR-1-200008745	Serial0/0/0:4	0.00%	0.00%	0 bps	0 bps
Customer X-eagan-MR-1-90302288	Loopback1	0.00%	0.00%	0 bps	0 bps
Customer X-eagan-VR-1-90302288	FastEthernet0/0.786	0.00%	0.00%	3801 bps	2311 bps
Customer X-fargo-VR-1-90302291	Serial0/1/0:14	0.00%	0.00%	0 bps	0 bps
Customer X-fargo-VR-1-90302291	Serial0/1/0:20	0.00%	0.00%	0 bps	0 bps
Customer X-fargo-VR-1-90302291	Serial0/1/0:5	0.00%	0.00%	0 bps	0 bps
Customer X-fortmyer-MR-2-90302289	Loopback1	0.00%	0.00%	0 bps	0 bps
Customer X-landolak-VR-1-200000071	GigabitEthernet0/0.110	0.04%	0.12%	469 Kbps	546 Kbps

Customer X-landolak-VR-1-200000071	Serial0/0/0:21	0.00%	0.00%	0 bps	0 bps

Exhibit E: Existing Client Projects (ECP)

Project Name:	Lab test for Performance Routing
Description:	**Issue:** Aurora (call center) BGP flap: Due to carrier maintenance, BGP can be impacted causing flapping which will result in service interruption. The Aurora location is 24/7 call center any interruption causes major impact. PFR will help to get a more controlled path selection and application-aware routing. Additionally, PFR will help to route traffic by choosing better path in event of circuit degradation at Data Center or any remote site. ***Benefits:*** Performance Routing (PfR) delivers intelligent path control for application-aware routing across the WAN. PfR provides: • Dynamic selection of the best path for application-based business policies • Application-based load balancing across paths for full utilization of bandwidth with improved network availability PfRv3 monitors application performance on a per-flow basis, and applies what is learned to select the best path for that application. Using smart-probe intelligence, flows are monitored passively; probes are sent only when specifically needed to further enhance efficiency. PfRv3 effectively load-balances across paths while delivering the best application-level SLA. PfRv3 represents the third generation of enhancements to Cisco's intelligent path control capabilities. It features simple, centralized configuration; improved application monitoring; higher scale; and faster convergence. PfRv3 innovations include the introduction of enterprise domains, a capability for service orchestration in the network that enables centralized configuration, automatic discovery, and single-touch provisioning. Simply define the domain, configure the hub site, and PfRv3 does the rest. Benefits: • Reduced WAN operating expenses • Full utilization of all WAN bandwidth by efficiently distributing traffic based on load, circuit costs, and path preference • Improved application performance with per-application best-path selection based on delay, loss, and jitter measurements • Improved application availability • Simple setup PfR is the technology for intelligent path control for Cisco Intelligent WAN, which builds upon four components: • Transport-independent design • Intelligent path control • Application optimization • Highly secure connectivity
Status:	In process

Exhibit F: Review Move Add Changes (RMAC)

RMAC Details	Ticket Opened	Ticket Type	Ticket State
Location X – enable Port 35 on Switch 7	4/6/15 2:48 PM	RMAC	Closed
Location X – Nursing Campus – schedule hot cut for BGP Timer Change	5/6/15 4:03 PM	RMAC	Pending
Customer X Data Center Data Center – inbound load sharing	6/29/15 2:49 PM	RMAC	Closed

Exhibit G: Critical Problem Reviews (CPR)

None for Q2 2015 quarter

Exhibit H: Ticket Management

Ticket #	Site Name - Issue	Ticket Opened	Impact
2015040110000159	Customer X, LLC- Bloomington -MAINTENANCE NOTIFICATION - 106466 -09 Apr 2015 3:00-7:00 am EST	4/1/2015 5:19	Moderate
2015040110000202	Customer X, LLC-Customer X Data Center Data Center -GigabitEthernet0/0/3 - DOWN CONNECTED TO CL Account# 61490432 Ckt ID ETH1000-16940138	4/1/2015 8:56	High
2015040110000579	Customer X, LLC- Aurora - RFO (wireless) [Resolved 24 hrs monitoring & auto close]	4/1/2015 13:11	High
2015040110000855	Customer X, LLC- Brooklyn Park Tech Center - **PEND Ufer, Maintenance Mode**	4/1/2015 16:13	High
2015040210000915	Customer X, LLC-Customer X Data Center Data Center - ASA 90% Memory Usage **Monitor**	4/2/2015 19:43	High
2015040310000191	Customer X, LLC- Fort Myers - SEC WIFI NOT WORKING [PND SE]	4/3/2015 8:08	High
2015040310000682	Customer X, LLC- Overland Park, KS - MR2 Alarm **Resolved 24hr close**	4/3/2015 15:48	Urgent
2015040410000126	Customer X, LLC- Mankato - MR1 down	4/4/2015 8:58	Urgent
2015040610000033	Customer X, LLC- Fargo- MR 2 alarm *PND EU*	4/6/2015 1:24	High
2015040610000408	Customer X, LLC- New Port Richey Network Down [Resolved]	4/6/2015 11:09	High
2015040610000711	Customer X, LLC- Fort Myers - Interface down [Resolved]	4/6/2015 13:28	High
2015040610000846	Customer X, LLC- Fort Myers - RMAC	4/6/2015 14:52	High
2015040810000495	Customer X, LLC- Land O' Lakes, FL**power outage**	4/8/2015 11:25	High
2015040910001214	Customer X, LLC-Customer X Data Center Data Center - Bandwidth Usage Alarm	4/9/2015 16:31	High
2015041310000734	Customer X, LLC- Fargo MR1 Down **pndg fp rfo**	4/13/2015 14:45	High
2015041310000743	Customer X, LLC- Moorhead - MPLS down [Resolved 24 hrs monitoring & auto close]	4/13/2015 14:52	High
2015041310000912	Customer X, LLC- Aurora - BGP Neighborship Drop - RFO	4/13/2015 16:59	Urgent
2015042010000293	Customer X, LLC- Denver - Primary MPLS Ethernet - Maintenance 30 Apr 2015 08:00 GMT	4/20/2015 10:33	High
2015042110000782	Customer X, LLC-Customer X Data Center Data Center - Interface down [Resolved]	4/21/2015 15:08	High
2015042110000791	Customer X, LLC-Customer X Data Center Data Center - Bandwidth Usage Alarm - GigEth0/0/3 [Resolved Utilization report attached]	4/21/2015 15:31	High

Exhibit J: Life-Cycle Management

End-of-Sale and End-of-Life Announcement for the Cisco 2800 Series Integrated Services Routers

Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end of sale and end of life of a product is distributed to the general public.	November 1, 2010
End-of-Sale Date	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	November 1, 2011
Last Ship Date: HW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	January 30, 2012
End of SW Maintenance Releases Date: HW	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.	October 31, 2014
End of Routine Failure Analysis Date: HW	The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.	October 31, 2012
End of New Service Attachment Date: HW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.	October 31, 2012
End of Service Contract Renewal Date: HW	The last date to extend or renew a service contract for the product.	January 30, 2016
Last Date of Support: HW	The last date to receive service and support for the product. After this date, all support services for the product are unavailable, and the product becomes obsolete.	October 31, 2016

Exhibit K: Monitored Device Inventory

Total Devices: xxx

Node	City
Customer X-appleton-CS-1-90302307	Appleton
Customer X-appleton-MR-1-90302307	Appleton
Customer X-appleton-MR-2-90302307	Appleton
Customer X-appleton-SW-2-90302307	Appleton
Customer X-appleton-VR-1-90302307	Appleton
Customer X-appleton-WC-1-90302307	Appleton
Customer X-appleton-WP-1-90302307	Appleton
Customer X-Aurora-IR-1-90302284	Aurora - DR
Customer X-aurora-MR-1-90302284	Aurora
Customer X-aurora-MR-2-90302284	Aurora
Customer X-aurora-SW-1-90302284	Aurora
Customer X-aurora-SW-2-90302284	Aurora
Customer X-aurora-VR-1-90302284	Aurora
Customer X-aurora-WC-1-90302284	Aurora
Customer X-aurora-WP-1-90302284	Aurora
Customer X-bismarck-CS-1-90302285	Bismarck
Customer X-bismarck-MR-1-90302285	Bismarck
Customer X-bismarck-MR-2-90302285	Bismarck
Customer X-bismarck-SW-11-90302285	Bismarck
Customer X-bismarck-SW-2-90302285	Bismarck
Customer X-bismarck-SW-3-90302285	Bismarck
Customer X-bismarck-SW-4-90302285	Bismarck
Customer X-bismarck-VR-1-90302285	Bismarck
Customer X-bismarck-WC-1-90302285	Bismarck
Customer X-bismarck-WP-1-90302285	Bismarck
Customer X-blaine-CS-1-90302305	Blaine
Customer X-blaine-MR-1-90302305	Blaine
Customer X-blaine-MR-2-90302305	Blaine
Customer X-blaine-VR-1-90302305	Blaine
Customer X-blaine-WC-1-90302305	Blaine
Customer X-blaine-WP-1-90302305	Blaine
Customer X-brandon-CS-1-90302610	Brandon
Customer X-brandon-MR-1-90302610	Brandon
Customer X-brandon-MR-2-90302610	Brandon
Customer X-brandon-SW-2-90302610	Brandon
Customer X-brandon-VR-1-90302610	Brandon
Customer X-brandon-WC-1-90302610	Brandon
Customer X-brandon-WP-1-90302610	Brandon

Glossary of Terms

Actual Incident Time	Defined by NetWolves is the length of time, from alert notification to resolution notification, as measured by the SRM²-S monitoring tool.
Availability	Measured at the device level by providing a percentage of time that NetWolves' monitoring systems are accessible from our NC² facility located in Tampa, Florida.
Business Hours	Hours of operation as defined by the customer and used to restrict the reporting window to reflect impact to the business.
Cisco General Deployment (GD)	Date at which this software release reached the "General Deployment" milestone in its lifecycle. A Major Release of Cisco IOS software reaches the "General Deployment" milestone when Cisco feels it is suitable for deployment anywhere in customer networks where the features and functionality of the release are required. Criteria for reaching the "General Deployment" milestone are based on, but not limited to, customer feedback surveys from production and test networks using the releases, CE bug reports, and reported field experience. Only Major Releases are candidates to reach the General Deployment milestone.
Cisco Major Release	A Major Release of Cisco IOS software delivers a significant set of platform and feature support to market. No new features, platform or interface support are added to a Major Release after its initial FCS to protect the stability of the release.
CPE Device	Customer-premises equipment or customer-provided equipment (CPE) is any terminal and associated equipment located at a subscriber's premises and connected with a carrier's telecommunication channel at the demarcation point ("DMARC "). The DMARC is a point established in a building or complex to separate customer equipment from the equipment located in either the distribution infrastructure or central office of the Communications Service Provider.
CPR (Critical Problem Review)	A service provided to MNO customers, who would present the following: a 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, and remediation steps to prevent the RFO from reoccurring.
DMARC	In telephony, the demarcation point is the point at which the public switched telephone network ends and connects with the customer's on-premises wiring. It is the dividing line which determines who is responsible for installation and maintenance of wiring and equipment.
ECP (Existing Client Projects)	An ECP is any work that will need to be completed which requires more than 8 hours designing and implementing by NetWolves SA/SD teams for an existing customer. ECP's have a dedicated project manager, lead engineer, and Account manager participation. All ECP will require a signed SoW and design document by the customer.

End of Engineering/Support	The date after which no scheduled maintenance releases will be produced for the major release. Releases which reach this milestone are still available through FSO and CCO for customers under maintenance contract or for CSE support until they reach the "End of Life" milestone.
End of Life	After this date, the software release is no longer officially supported by CSE and is removed from CCO. Please note that Cisco IOS software releases typically reach the "End of Life" milestone three years following FCS of the major release. Specific "End of Life" dates are determined on a case-by-case basis.
End of Sale	After this date, the software release may no longer be ordered. Releases which reach this milestone are still available through FSO and CCO for customers under maintenance contract or for Customer Service Engineering (CSE) support until they reach the "End of Life" milestone.
IM (Incident Management)	The processes and procedures created to identify, analyze and correct current and potential customer affecting issues to restore normal customer functionality and minimize customer downtime. Incident tickets are created to troubleshoot and track customer affecting outages or issues from inception to resolution. These tickets are the primary method of communication to our customers regarding the status of their outage or issue. Urgent: site is down; no connectivity, failover was unsuccessful or NetWolves declares an emergency. High: site is functioning in a degraded state or has failed to back up circuit and business has been minimally impacted. Moderate: site is functioning in a degraded state but still operational (i.e. slowness/packet loss/circuit bounce and restored in under 2 minutes), or operating with one circuit in a bond inoperable (i.e., bonded T1, bonded broadband.
LEC	Local Exchange Carrier (LEC) is a regulatory term in telecommunications for the local telephone company.
Network Facility Provider	an entity that owns or operates facilities such as satellite earth stations, broadband fiber optic cables, telecommunications lines and exchanges, radio communications transmission equipment, mobile communications base stations, and broadcasting transmission towers and equipment, which provide access to a network.

Network Node Performance (NNP)	Network Node Performance (NNP) – information and metrics about the operational resources of a specific node which are captured and recorded.
NHQ (Network Holistic Quality)	NetWolves measures the holistic quality of a network (NHQ) by sampling and/or reporting on the following categories: By aggregating these metrics, we can provide our customers with true insight into their infrastructures and show value add in our services.
Obsolete	After this date, the maintenance release is no longer orderable and is removed from CCO. The term "obsolete" generally refers to a maintenance release within a major release train. Because our cumulative fix model is designed to improve quality with every release, obsolete maintenance releases are generally replaced by newer maintenance releases within the same or more recent major release train. Obsolete versions cannot be ordered on new systems or as spares but can temporarily be made available via CCO under certain conditions. If an obsolete version is made available to a customer, the customer will be expected to maintain master copies of such images they may need in the future. Obsolete software releases are eligible for CSE support until they reach the "End of Life" milestone as previously described.
PE Device	A Provider Edge router (PE router) is a router between one network service provider's area and areas administered by other network providers
RMAC (Reviews, Moves, Adds & Changes)	An RMAC is any work that will need to be completed which requires less than 8 hours designing and implementing by NetWolves SA/SD teams for an existing customer. RMAC's do not require any type of project management and are not additional billable items but are simply included as part of NetWolves managed services.
TTR (Time To Resolution)	as defined by NetWolves is the length of time, from event notification, either by customer or monitoring tool, to issue resolution, as verified between the customer and a NetWolves NC^2 (Network Command and Control) technician, and follow-up troubleshooting/Reason For Outage information.
Utilization	Primarily based on WAN circuit utilization as this is almost always the throughput bottleneck of a network. Even so, all primary transport path or "Backbone" interfaces will be monitored by default for NetWolves' MNS customers.

NetWolves

NetWolves Network Services
4710 Eisenhower Blvd.
Building E-8
Tampa, FL 33634
(813) 579-3200