TEST REPORT

Tolly.

#212101
February 2012
Commissioned by
Meraki, Inc.

Meraki MX90 Cloud Managed Security Appliance

WAN Optimization Performance Evaluation

Executive Summary

Meraki's MX90 Cloud Managed Security Appliance integrates firewall, VPN and WAN optimization in one cloud-managed solution that allows growing enterprises to manage up to hundreds of branch routers in a multi-site network from one intuitive Web-based interface. While testing focused on WAN optimization performance, Meraki notes that the MX90 implements an extensive feature set including WAN optimization, site-to-site VPN, integrated traffic shaping and built-in anti-virus, anti-phishing, and content filtering.

The evaluation of Meraki's MX90 focused on file transfer performance of FTP, HTTP, and CIFS protocols. Tolly engineers found the Meraki MX90 Cloud Managed Security Appliance significantly improves transfer time by up to 209X in "warm" (cached) runs across protocols under test compared to the baseline (non-cached). See Figure 1.

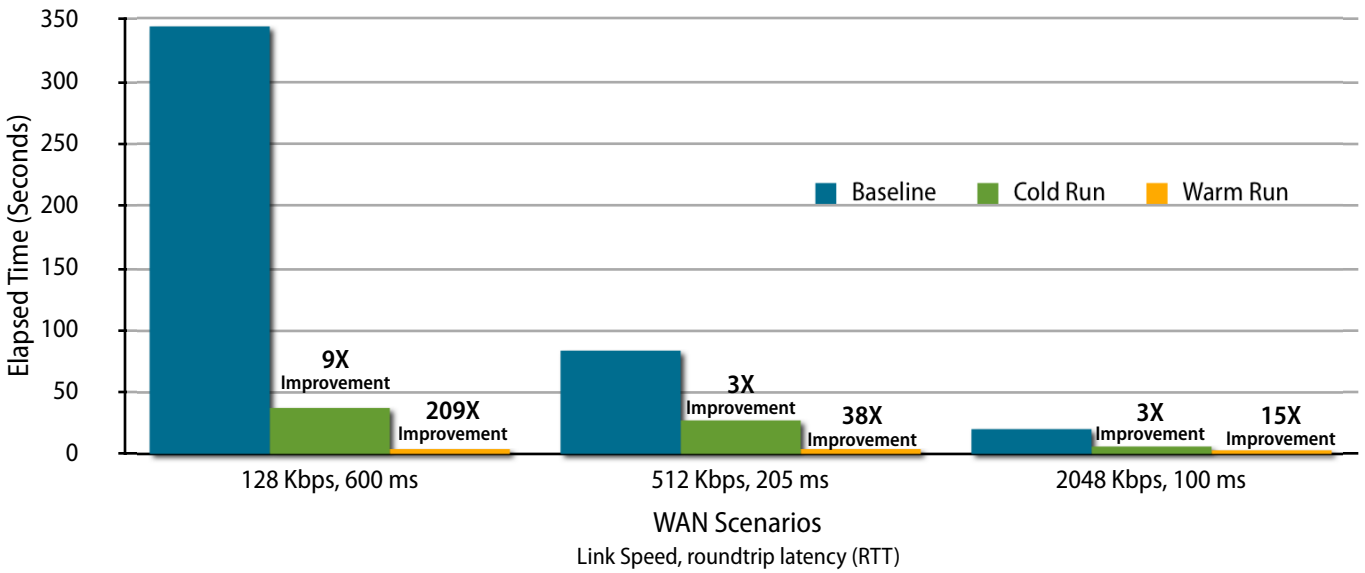
The Bottom Line

The Meraki MX90 Cloud Managed Gateway:

1. Can improve FTP performance by up to 209X
2. Can improve HTTP performance by up to 45X
3. Can improve CIFS performance by up to 16X

FTP WAN Transfer Time & Improvement Over Baseline

Lower bars are better



Notes: The number shown on the bar indicates how many times faster a given run was compared to the baseline run. Simulated links were symmetrical. "Baseline" denotes a run without the Meraki appliance optimizing data transmission over a WAN link. "Cold Run" represents the first attempt by the Meraki MX90 to accelerate the WAN connection for the specific data stream being transmitted. The "Warm Run" represents subsequent attempts to transmit data streams previously accessed over the WAN link, which build upon the "cold" run's WAN optimization and compression, and can leverage data segments cached locally to rebuild the file.

Source: Tolly, December 2011

Figure 1

Background

Organizations face many challenges with managing distributed networks, controlling connectivity costs, and ensuring performance at remote locations. Meraki's MX Cloud Managed Security Appliances make it easy and affordable for network administrators to deploy multi-service devices across a distributed network and ensure application performance at remote sites. Meraki, Inc. commissioned Tolly to evaluate the WAN optimization and performance of their MX90 Cloud Managed Security Appliance.

A commercial-grade WAN emulator was used in the test environment to emulate several real-world bandwidth scenarios commonly used in distributed networks and at branch/ remote locations. A pair of MX90 Cloud Managed Security Appliances were used to accelerate traffic between the data center and remote branch location.

Performance Test Results

Tolly engineers demonstrated the Meraki MX90 Cloud Managed Security Appliance improves application performance and can reduce bandwidth consumption, thus allowing branch offices to avoid costly bandwidth upgrades while accelerating application performance for a number of protocols.

For all application traffic tests, engineers conducted a baseline measurement test (without the Meraki appliance optimizing data transmission over a WAN link), a "cold" run and a "warm" run across a range of bandwidth/latency settings: a simulated 128-Kbps link with 600 milliseconds of latency or roundtrip time (RTT), a simulated 512-Kbps

Meraki, Inc.

MX90 Cloud Managed Security Appliance

WAN Traffic Optimization and Performance

Tolly Certified

Tested December 2011

Detailed Test Results

Transfer Times by Protocol Bandwidth Scenario

Protocol/ Bandwidth	Baseline (s)	Cold Run (s)	Warm Run (s)	Cold Run Improvement Multiple	Warm Run Improvement Multiple
CIFS v1					
128 Kbps, 600 ms	671.17	304.55	67.27	2.2	10
512 Kbps, 250 ms	172.88	72.34	18.64	2.4	9.3
2048 Kbps, 100 ms	41.61	17.83	5.28	2.3	7.9
CIFS v2					
128 Kbps, 600 ms	725.41	307	47.54	2.4	15.3
512 Kbps, 250 ms	164.48	70.62	10.39	2.3	15.8
2048 Kbps, 100 ms	40.99	17.83	5.28	2.3	7.8
FTP					
128 Kbps, 600 ms	344.93	37.96	1.65	9.1	209
512 Kbps, 250 ms	83.82	28.13	2.19	3	38.3
2048 Kbps, 100 ms	20.97	6.93	1.32	3	15.9
HTTP					
128 Kbps, 600 ms	73.85	37.58	1.62	2	45.6
512 Kbps, 250 ms	17.91	9.99	0.76	1.8	23.6
2048 Kbps, 100ms	4.38	2.36	0.36	1.9	12

Source: Tolly, December 2011

Table 1

link with 250 milliseconds of RTT, and a simulated E-1 connection (2048 Kbps) with 100 milliseconds of RTT.

The "cold" run represents the first attempt by the Meraki MX90 to accelerate the WAN connection for the specific data stream being transmitted. That is, the Meraki device has not processed this data stream previously and, thus, does not have any packet segments cached locally at the target site. However, the cold run transfer is accelerated using compression and protocol optimization techniques.

Subsequent attempts to transmit data streams previously accessed over the WAN link result in "warm" runs, which build upon the "cold" run's WAN optimization and compression, and can leverage data segments cached locally to rebuild the file, resulting in fewer bytes transmitted across the WAN link, fewer client-server round trips, and greater effective throughput perceived by the remote user.

Given that "warm" run transfers represent the majority of use cases (all file transfer events for a given file except the first), the MX90 Cloud Managed Security Appliances offer a significant improvement in effective WAN link capacity.

FTP

Engineers tested transfer times of files using FTP from a Windows 2008 Server to a Windows client PC. The test was conducted over three bandwidth scenarios, 128 Kbps, 512 Kbps and 2048 Kbps, and repeated at least three times to establish an average.

Engineers tested the effect of the Meraki MX90's WAN optimization on FTP traffic across the three WAN scenarios described above. When averaging the time transfer across the three bandwidth scenarios, "cold" run results demonstrate that the MX90 delivered, almost 10 times faster transfer time than the unaccelerated baseline WAN environment results. In "warm" runs, the Meraki MX90 delivered the data an average of 87 times faster than the baseline across the three WAN bandwidth scenarios. See Figure 1 and Table 1.

HTTP (Web Traffic)

Engineers also tested the effect of the Meraki MX90's WAN optimization on HTTP traffic across the three WAN scenarios described above. When averaging the time transfer across the three bandwidth scenarios, "cold" run results demonstrate that the MX90 delivered, on average, almost three times faster file transfer time than the unaccelerated baseline WAN environment results. In "warm" runs, the Meraki MX90 delivered up to 45 times faster file transfers over the baseline results. See Table 1.

CIFS (Microsoft Windows File Sharing Protocol)[1]

Engineers also tested the Common Internet File System(CIFS) traffic, which is the protocol underlying Microsoft's Windows file sharing system. Testing was executed using a "copy" command that triggered the CIFS protocol transfer. When a Windows 2003 Server was used to serve the test files, the file transfers used CIFS protocol version 1, whereas file transfers served by the Windows Server 2008 used CIFS protocol version 2.

Tests across the three bandwidth scenarios demonstrated that, during "cold" run transfers, the MX90 delivered file transfers nearly twice as fast, on average, as the unaccelerated baseline. This was demonstrated using either CIFS version 1 or version 2. The "warm" runs under the same test scenarios, showed the Meraki MX90 delivered up to 10X faster file transfers over the baseline, when using CIFS version 1, and up to 15X faster using CIFS version 2. See Table 1.

Analysis

Test results show that the MX90 Cloud Managed Security Appliances provide powerful bandwidth optimizations that dramatically reduce the amount of data that is transmitted across the WAN, and more importantly, accelerate the file-transfer throughput using FTP, HTTP or CIFS (Windows file shares).

In addition to reducing the amount of data traversing the WAN, the MX90 also provides a built-in firewall, layer 7 application traffic shaping, IPsec VPN technology for securing site-to-site traffic, WAN link bonding and advanced content and security filtering.

Test Bed Configuration

Tolly tested two Meraki MX90 Cloud Managed Security Appliances running software build: T-76568M-g1724d4e8-jbicket.

The MX90s tested were configured with five front-panel GbE ports, one GbE mirror port, one GbE management port, and one GbE port for WAN connectivity. The MX90s at either end of the WAN link established an encrypted IPsec VPN tunnel to secure the site-to-site traffic (split-tunnel mode).

The built-in firewall on the MX90s were configured to scan all traffic using simple rules to block all inbound non-router traffic, while allowing all outbound traffic. Other features like traffic shaping, security scanning, content filtering etc. were not enabled for the duration of the test.

As shown in Figure 2, the test network consisted of a pair of MX90 appliances deployed across a WAN connection simulated by an Apposite Linktropy Mini2 WAN emulator. The WAN link scenarios used are listed in the test methodology section of this report.

[1] Formerly known as Server Message Block (SMB)

Engineers used two servers to host the test files. The first server ran a Microsoft Windows 2003 Standard Edition (Service Pack 2) operating system, and was equipped with an AMD Athlon64 X2 3800+ Dual Core CPU running at 2 GHz, with 2GB RAM. This server hosted an SMB file server to serve test files using CIFS protocol (version 1).

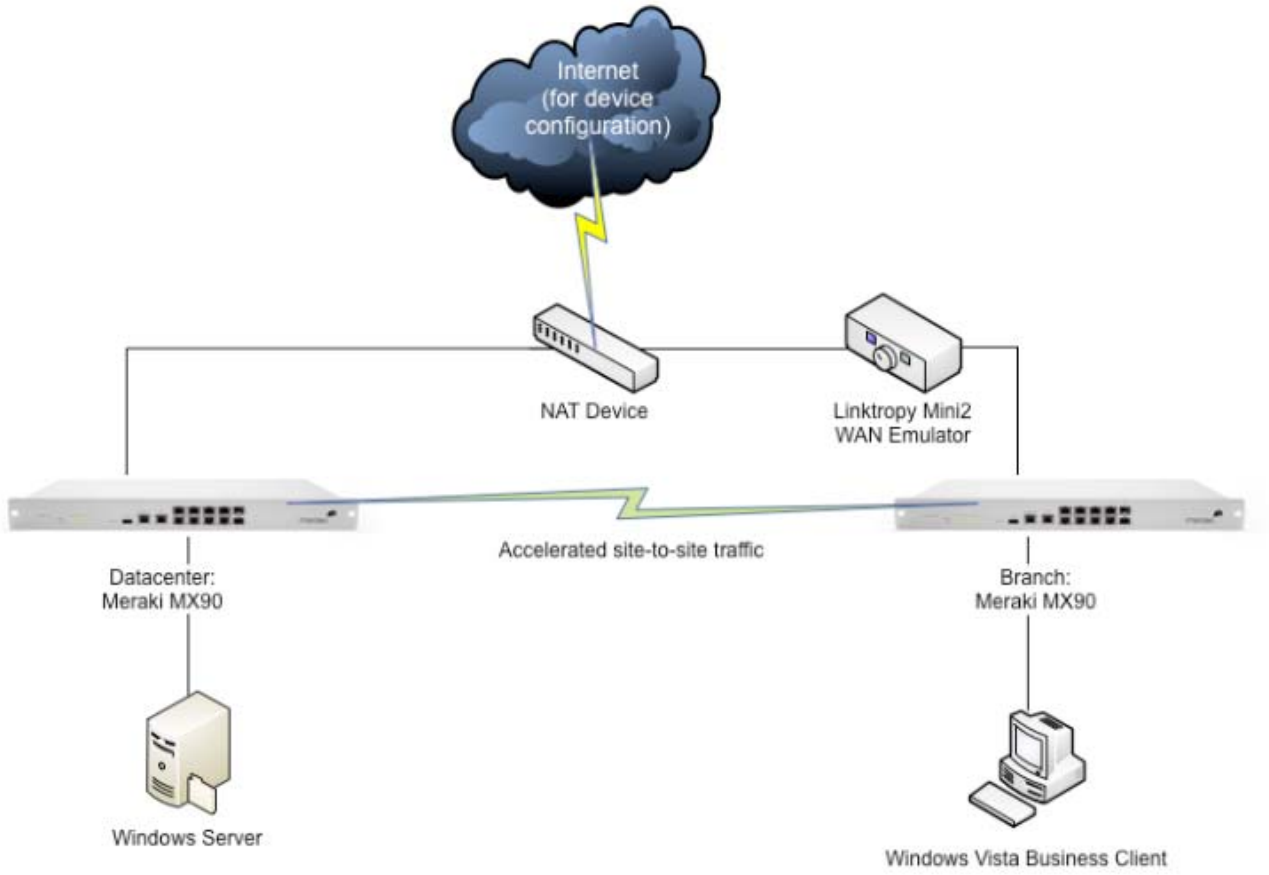
The second test server ran Microsoft Windows Server 2008 Standard (Service Pack 2), on Intel Core™2 Duo E6320 running at 1.83 GHz, with 3 GB RAM. This server hosted an SMB file server to serve test files using CIFS protocol (version 2), an FTP server and a Web Server.

The client PC ran Microsoft Windows Vista Business Edition (Service Pack 2), and was equipped with an Intel Core2Duo P8600 CPU running at 2.4 GHz, and 3 GB RAM.

Test traffic across the WAN links was generated when the client PC on one end requested a set of test files of different sizes from a test server at the other end of the WAN link. From the point of view of the client and the server, the communication was transparent, meaning that they were not aware of the presence of the MX90 Cloud Managed Security Appliances.

The management interfaces of the Linktropy Mini2 WAN emulator and the two MX90s were all connected to a Meraki MX60 Cloud Managed Security Appliance to provide Network Address Translation (NAT) in the DMZ and to provide Internet connectivity for the management interfaces of the MX90s.

Test Bed Topology



Source: Tolly, December 2011

Figure 2

Test Methodology

The aim of the test methodology used was to show the performance benefits of using Meraki's WAN optimization technology in the MX90s to reduce the amount of data transferred across secure WAN links between different sites. Tests were architected to illustrate such benefits while handling medium to large test files using CIFS, FTP and HTTP protocol across WAN links of various bandwidths and round-trip latency. For each protocol tested, the corresponding client and server programs were running on the client and server end-stations. The test files used for each test are shown in Table 2 below.

The Linktropy Mini2 WAN Simulator was configured to emulate a WAN link with a bandwidth and latency as appropriate for the specific test permutation. Three WAN scenarios were tested: 128 Kbps with 600 ms RTT, 512 Kbps with 250 ms RTT, and 2,048 Kbps with 100 ms RTT. A Perl script measured the time taken to complete a transaction.

For the baseline run, the MX90 appliances did not accelerate the WAN traffic, but rather acted as pass-through devices, allowing the client and server to communicate over an unaccelerated WAN link. The time taken to complete the transaction was recorded.

In the "cold" and "warm" runs, the MX90s actively processed and accelerated traffic across the WAN link. When the client sent a request to the server (using CIFS, FTP or HTTP protocols), the MX90 on the server side accelerated the server's response to minimize the amount of data transferred on the WAN link.

In the "cold" run, the MX90 data compression and protocol-based optimization on the traffic sent over the WAN link. The time taken to complete the transaction was recorded.

The subsequent transfer, the "warm" run takes significantly less time for the second pass, since previously cached data can be used to minimize data transfer. A "warm" run was performed where the same, unaltered files were again accelerated by MX90 appliance, and the time taken to complete the transaction was noted.

After the "cold" and "warm" runs, the cache of the MX90s were flushed by issuing a command from the management console, and then rebooting the appliances to remove any previously built caches. Engineers then ensured that the Windows client did not contain a cached copy of the test file.

These steps were repeated for the different test permutations by varying the file size to be transmitted, the bandwidth and latency settings of the WAN link. Each test was repeated three times to ensure repeatability of the results, and the average of the three runs was published as the final number.

TOLLY™ common TEST PLAN SERIES

The test methodology used for this report relies upon test procedures, metrics and documentation practices as defined in Common Test Plan #1208: Remote File Caching Performance.

To learn more about Tolly Common Test Plans, please visit: www.tolly.com

Test Files and Their Sources

Test Name	Test File	Size	Description	Source
CIFS v1, and CIFS v2	S4nw3.dwg	2066 KB	CAD drawing file	http://www.augi.com/images/uploads/content/AUGIGauge.zip.
CIFS v1, and CIFS v2	SITE3D.dwg	9127 KB	CAD drawing file	http://www.augi.com/images/uploads/content/AUGIGauge.zip.
FTP	bible.txt	3953 KB	The King James version of the bible	http://corpus.canterbury.ac.nz/descriptions/large/bible.html
FTP	E.coli	4530 KB	Complete genome of the E. Coli bacterium	http://corpus.canterbury.ac.nz/descriptions/large/E.coli.html
HTTP	pic	501 KB	Black and white fax picture	http://corpus.canterbury.ac.nz/descriptions/calgary/pic.html
HTTP	pi.txt	977 KB	The first million digits of pi	http://corpus.canterbury.ac.nz/descriptions/misc/pi.html

Source: Tolly, December 2011 Table 2

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services. You can reach the company via E-mail at sales@tolly.com, or via telephone at +1 561.391.5610.

Visit Tolly on the Internet at: http://www.tolly.com

Test Equipment Summary

The Tolly Group gratefully acknowledges the providers of test equipment/software used in this project.

Vendor	Product	Web
Apposite Technologies	Linktropy Mini2 WAN emulator	http://www.apposite-tech.com/products/mini2.html

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

212101-Ndljomfz2-kk-mts-kt-2012-02-21-VerL1