Unified Threat Management
Comparative Throughput Performance

WatchGuard Firebox M270

Cisco Meraki MX84

Fortinet FortiGate 100E

SonicWall NSA 2650

Sophos XG 210

2 August 2018

DR180622E

Miercom.com

www.miercom.com

Contents

Executive Summary

Unified Threat Management (UTM) appliances are a consolidated security product with routing, firewall, intrusion prevention, antivirus, Virtual Private Network (VPN) and other protective measures for small to mid-size business networks. While these devices carry the power and functionality of a next generation firewall and secure web gateway, the performance has traditionally been impacted by intensive traffic processing. By testing performance of across a variety of UTM products, it creates an objective view of processing advantages and shortfalls, thereby allowing manufacturers to best optimize their products.

Miercom was engaged by WatchGuard Technologies, Inc. to conduct an independent, comparative performance assessment of its Firebox M270 against similar leading UTM network security appliances: Cisco Meraki MX84, Fortinet FortiGate 100E, SonicWall NSA 2650 and Sophos XG 210. All products were exposed to increasing traffic loads, with different protocols, while evaluating the impact on network performance. When identifying competitive equipment for this report, selected rack mount appliances were those closest in price (MSRP) to the Firebox M270. In each case this required models to be included that had a closer equivalent price to the WatchGuard Firebox M370.

Product comparisons were made using the following scenarios: firewall, additional security features and full UTM mode. Firewall performance measured transport and application network layer traffic. Then security features were individually enabled to evaluate the impact on performance for HTTP and HTTPS loads. Finally, the full set of security functions was enabled (firewall, intrusion prevention system, antivirus and application control) over HTTP and HTTPS.

Key M270 Performance Findings

- Outperforms more costly competitors' models with security running
- Highest realistic IMIX UDP performance of 1.5 Gbps and 4.7 Gbps for 1518-byte frames
- Highest UTM HTTP throughput at 1.2 Gbps, outperforming vendors by at least 48%
- Superior encrypted UTM throughput at 661 Mbps, surpassing closest competitor by 11%

Based on results of our testing, the WatchGuard Firebox M270 displayed exceptional performance, outperforming its competitors for stateless and stateful traffic throughput scenarios with different firewall features enabled. Its high-rate performance with security features enabled earns it the *Miercom Performance Verified* certification.

Robert Smithers
CEO
Miercom

Introduction

Unified Threat Management devices are an evolving class of network edge security platforms that incorporate and perform multiple security functions in a single appliance. The devices tested for this report all address and incorporate the following security functions:

Security Function	Acronym	Description
Firewall	FW	Controls and filters the flow of traffic, providing a relatively low-level barrier to protect a trusted internal network from an unsecure network (such as the Internet).
Intrusion Prevention System	IPS	Monitors all network activity, looking for malicious behavior based on known-threat signatures, statistical anomalies, or stateful protocol analysis. If malicious or highly suspicious packets are detected, they are identified, logged, reported and, depending on IPS settings, automatically blocked from access to the internal network.
Application Control	AppCtrl	Enforces policies regarding security and resources (network bandwidth, servers, etc.) by restricting or controlling which application traffic can pass through the UTM, usually in either direction. Security-wise, Application Control is intended to reduce occurrences of infection, attacks and malicious content.
Hypertext Transfer Protocol Proxy/Antivirus	HTTP Proxy/AV	The security appliance is a proxy for HTTP traffic. This is where a client issues a "get" request and retrieved files are buffered in memory in the security appliance. Files are then sent to an antivirus engine that looks for viruses and removes packets containing malicious content. Proxy-based virus and content scanning is a more secure and accurate method than stream-based inspection of client/server traffic. With Proxy/AV scanning is performed during the handshake of data transfer.
Hypertext Transfer Protocol Secure	HTTPS	The security device responds to incoming encrypted connection requests on the secure socket layer (SSL), and then actively scans and blocks packets containing malicious content, like HTTP/AV processing. The HTTPS encryption/decryption process places an appreciable load on the security device that directly impacts its overall throughput rate.
Unified Threat Management	UTM	An all-inclusive security setting, where multiple functions are performed by the same, single security device. The functions typically include: firewall, IPS, AV, VPN (control of virtual private network tunnels), content filtering, and sensitive data loss prevention.

While security is certainly important, it does place a load on network performance. This report documents the effect of security on data throughput for each UTM device. Knowing the impact security places on performance can help IT departments decide on the best fit for their business from similar network security products.

Products Tested

Product	Firmware Version
WatchGuard Firebox M270	Build: 12.2.B563533 (beta)
Fortinet FortiGate 100E	5.6.4 B1575
Meraki MX84	13.28
SonicWall NSA 2650	6.5.1.1-42n
Sophos XG 210	SFOS 17.0.0 GA MR-8

WatchGuard Firebox M270

The *Firebox M270* is the latest and powerful offering in WatchGuard's Firebox UTM series. It offers enterprise-grade security to small and mid-size businesses with eight 1-GE ports. Its firewall throughput is specified to reach a maximum of 5 Gbps.

This model uses the newest generation of Intel Atom processors, with Intel Quick Assist Technology (Intel QAT) for high performance hardware-based security acceleration. This provides optimum performance of network traffic, including HTTPS content inspection and faster throughput in VPN tunnels.

Supported security features include: firewall, virtual private networking with SSL and IPSec, intrusion prevention, application proxies for various protocols (HTTPS, HTTPS, SMTP, DNS and others) and antivirus. Routing is policy based, and reporting is simple.

SonicWall Network Security Appliance (NSA) 2650

The *SonicWall NSA 2600* is a simple but effective next generation firewall for securing small businesses, branch offices and campuses. Its eight 1-GE ports support a firewall throughput of up to 1.9 Gbps.

Supported security features include: deep packet inspection firewall, stateful packet inspection firewall, application intelligence and control, intrusion prevention, antivirus, antispyware, content and URL filtering and SSL inspection.

Fortinet FortiGate 100E

The *FortiGate 100E* is an enterprise-grade firewall solution for unified security and policy management. There are twenty ports – 2 WAN, 1 DMZ, 1 Management, 2 High Availability, and 14 Switch ports. It is specified to provide throughput of up to 7.4 Gbps for firewall, 500 Mbps for IPS and 360 Mbps for UTM.

Supported security features include: firewall policies, virtual private networking with SSL and IPSec, intrusion prevention, application control and next generation firewall.

Meraki MX84

The *Meraki MX84* is a UTM solution for medium sized branch office networks. This cloud-managed product includes SD-WAN capabilities and a 500 Mbps stateful firewall performance, as well as a 320 Mbps throughput UTM protection.

Supported security features include: firewall policies, virtual private networking with SSL and IPSec, intrusion prevention, application control and next generation firewall.

Sophos XG 210

The *Sophos XG 210* firewall provides a unified management system to create policies based on user and applications for powerful network protection, with six ports to support up to 14 Gbps of firewall throughput and 1.7 Gbps next generation firewall performance.

Supported security features include: firewall, virtual private networking, intrusion prevention, application control, web filtering and antivirus.

How We Did It

Miercom used hands-on testing designed to simulate real-world threat environments, providing a robust, realistic assessment of product capability and effectiveness. Testing identifies the strengths and weaknesses of each Device Under Test (DUT).

The methodology was intended to validate product specifications regarding UDP, HTTP and HTTPS traffic flow processing. Realistic UDP, HTTP and HTTPS traffic flows were produced and circulated through the test network, acting as typical client-server requests and file transfers.

To determine the impact of security measures on performance, each DUT was analyzed for data throughput with individual features enabled. In some cases, devices are unable to disable firewall inspection, so this fundamental security layer was tested first. This low-level process represents the highest achievable throughput for each UTM product. As additional security services are enabled, the performance is compared to the firewall throughput to determine the impact of protection.

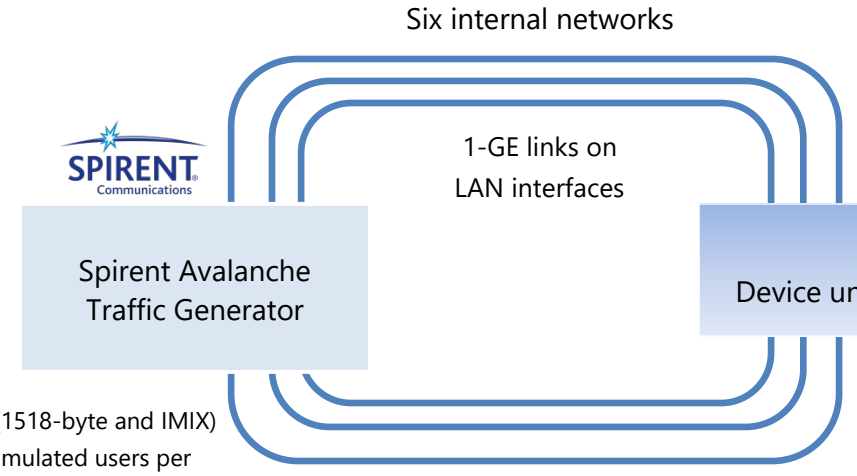
Throughput is just one useful metric when implementing network security appliances in a business environment; security is equally important. But network performance impact helps IT departments make a practical choice between similar, highly secure network appliances.

Test Tools

Source: Miercom

Some of the test tools featured above are used for real-time traffic generation, traffic monitoring and data capture throughout testing. During testing, the Spirent C100-S3 (v4.85) was used to generate traffic loads and collect throughput data.

Test Bed Diagram



- UDP (1518-byte and IMIX)
- 100 simulated users per interface with 100 HTTP/HTTPS GET requests per user, retrieving the same 1 MB .dat (binary) file

Source: Miercom

For the UDP performance test, we used Spirent Test Center; for stateful traffic, we used Spirent Avalanche. When testing the Meraki MX84, we used a switch between the trust and trusted sides of the network, as it requires cloud access to work.

External client traffic was sent from the Spirent Test Center or Avalanche to each DUT using three 1-GE links to three ingress LAN ports, and server responses were received via three 1-GE links to three egress LAN ports, for a total of six interfaces. Traffic represented real-world, high-stress network activity by using client-server connections of both stateless UDP and stateful HTTP/S traffic.

For initial firewall tests, stateless UDP and stateful HTTP and HTTPS traffic were used.

For stateless traffic, 250 bidirectional discrete flows of UDP packets were sent on all six 1-GbE interfaces, delivering a total of 6 Gbps to and through the DUT. This was sent in two loads for two separate tests:

1. UDP with all large, 1518-byte packets
2. UDP with IMIX of 66-byte (60.7 percent), 594-byte (23.7 percent) and 1518-byte (15.7 percent) packets for a total of 10,000 packets

Throughput for each DUT was observed for the maximum rate in megabits per seconds (Mbps) before a single packet was lost. Results are featured on page 11.

For stateful traffic, there were 100 users on the client side sending an HTTP GET request to download 1 MB binary .dat file from 100 simulated servers. There were 100 GET requests per user on the client side. This procedure was followed for both:

1. HTTP
2. HTTPS using ECDHE-RSA-AES128-GCM-SHA256
3. HTTPS using AES256-SHA256 for SonicWall only (does not support the above cipher suite)

Throughput was observed for its maximum rate in Mbps before any transaction of file transfer failed. This testing was repeated for each DUT with additional individual security services enabled and with full UTM mode. Performance was compared to the firewall throughput to determine the effect the security service has on each DUT.

Stateful throughput using HTTPS was tested with decryption capabilities enabled. However, the Sophos XG 210 required enablement of at least one security feature. In Sophos' case, any configuration with decryption required that AV was also enabled. Therefore, HTTPS FW only performance for Sophos is not available. Additionally, the performance of HTTPS with IPS only enabled for Sophos was not available, as it would automatically require AV enablement. Cisco Meraki does not support any HTTPS decryption/proxy and was not tested.

Results are detailed on pages 13-14 to maintain fair comparisons.

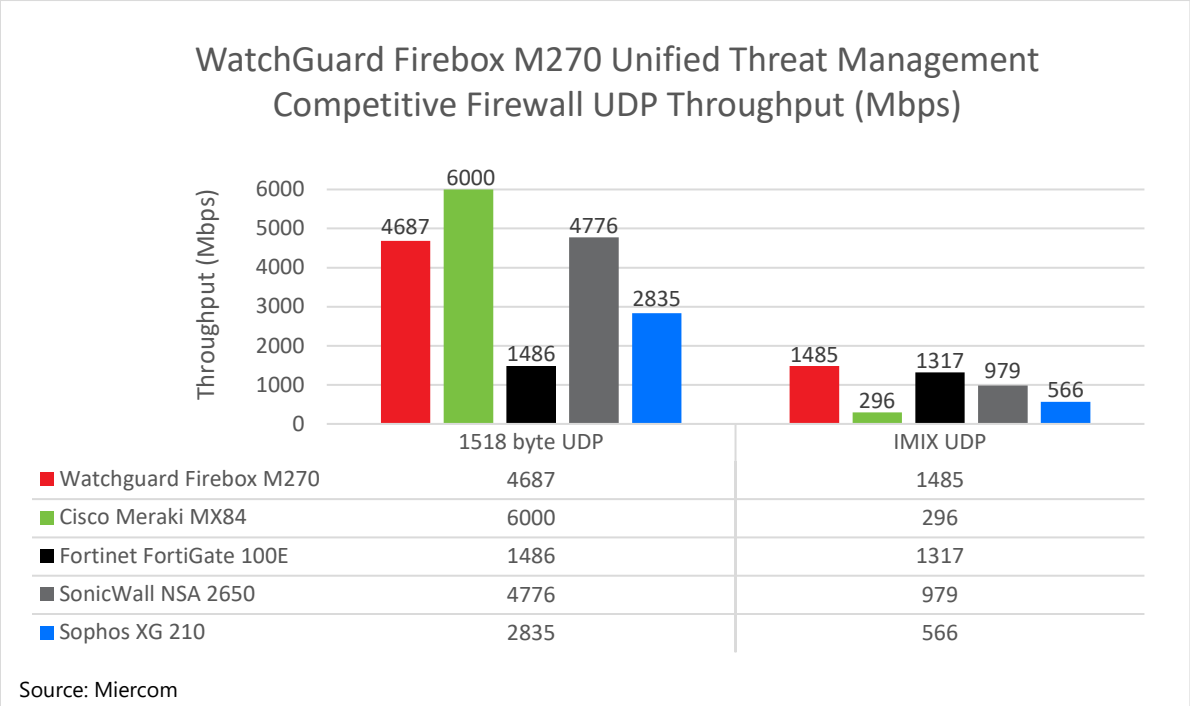
Performance Testing

Stateless UDP 1518-Byte and UDP IMIX Throughput

This test measured the maximum rate of traffic of the security appliance under test in Mbps. Only the firewall security service was enabled since it is the most basic and fundamental service of a security appliance.

For the first test, stateless bidirectional UDP 1518-byte packets were sent on all six interfaces for a maximum of 6 Gbps of traffic. Then the second stateless traffic test used bidirectional UDP IMIX traffic, wherein the packet size varied using the following distribution: 60.7 percent small packets (66-byte), 23.7 percent mid-sized packets (594-byte), and 15.7 percent large packets (1518-bytes).

Chart 1: Unified Threat Management Throughput for Stateless UDP Traffic



Source: Miercom

Stateless UDP traffic was generated to determine the firewall packet routing capabilities of each product. The DUT used 6x1GbE ports, where three were ingress from client to server and the other three were egress from server to client. Maximum line rate performance was 6 Gbps. For 1518-byte packets, the WatchGuard Firebox M270 achieved 94.5 percent of its expected maximum throughput of 4.96 Gbps. This UTM outperformed Fortinet by 68.3 percent and Sophos by 39.5 percent. While the Cisco Meraki achieved full line-rate performance for 1518-byte traffic, WatchGuard had the highest throughput for realistic IMIX traffic at 1.5 Gbps.

Stateful Throughput (HTTP/HTTPS)

Most Internet traffic uses the stateful Layer-7 application protocol HTTP to establish client-server connections over Layer-4 Transmission Control Protocol (TCP). Networks can upload and download files from the public Internet using HTTP, requiring high-level processing and inspection for malicious content.

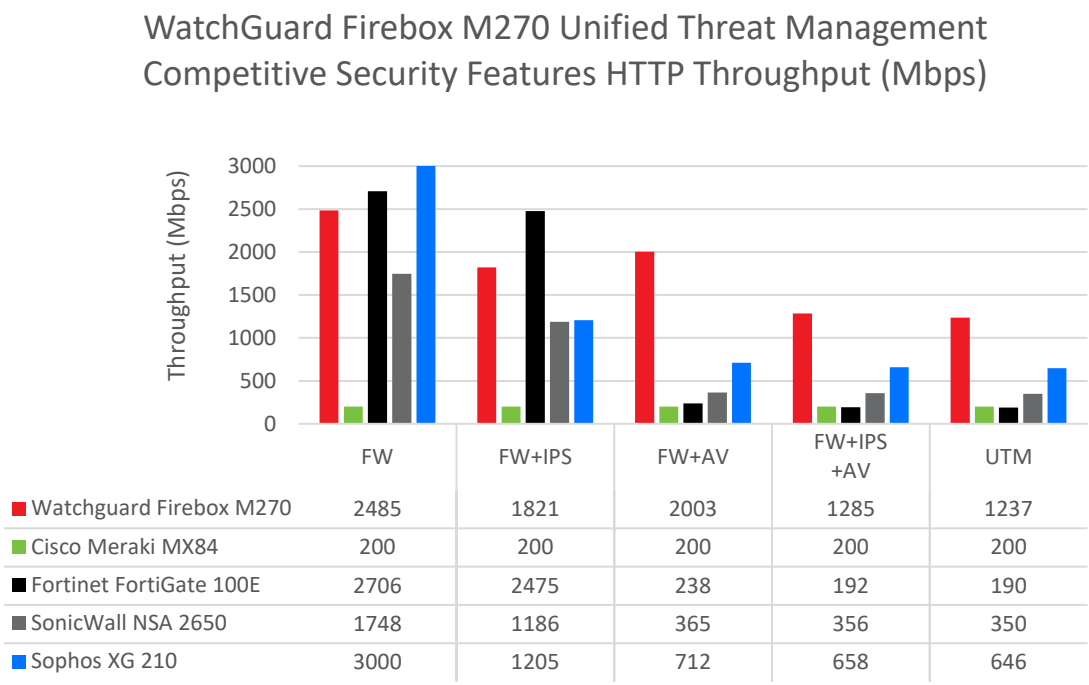
The most basic inspection is done using a firewall, with additional security services available from vendor to vendor. The most popular services include: decryption, IPS, AV and application control. The test results below reflect similar security appliances with firewall and decryption enabled as an initial test, and additional security features applied using the following configurations:

1. **FW.** Only the firewall was enabled to HTTP traffic stream.
2. **FW + IPS.** IPS was enabled, in addition to the firewall.
3. **FW + AV.** Web/HTTP proxy and AV processing was enabled, in addition to the firewall. Prior to the performance testing of this configuration scenario, a special test virus look-alike, called EICAR, was included in the files sent to ensure the appliance's antivirus processing was appropriately configured, scanning files and flagging viruses.
4. **FW + AV + IPS.** AV and IPS were enabled, in addition to the firewall.
5. **Full UTM.** Where the appliance's AV, IPS and Application Control were all concurrently enabled and applied, in addition to the firewall.

The Spirent Avalanche generated increasing loads of HTTP test traffic over three pairs of interface where 100 simulated clients per interface launched 100 GET requests to 100 simulated servers, resulting in a download retrieval of 1 MB binary file. Client and server sides were separated by different LANs.

Similarly, stateful HTTPS traffic loads were sent through the DUT using the configuration and test setup. The ECDHE-RSA-AES128-GCM-SHA256 encryption standards were used to secure traffic on the application layer with HTTPS, except for SonicWall as it does not support that cipher suite. We used AES256-SHA256 for SonicWall only. When the 1 MB binary file was requested, each packet was decrypted and re-encrypted before transfer. This processing was expected to place a load on the security appliance and throughput. The importance of encrypted traffic is to combat security threats, but attackers commonly use this very countermeasure to obfuscate malware until it reaches its destination. Each DUT should be capable of examining encrypted messages without severely degrading its throughput.

Chart 2: Unified Threat Management Throughput for Stateful HTTP Traffic

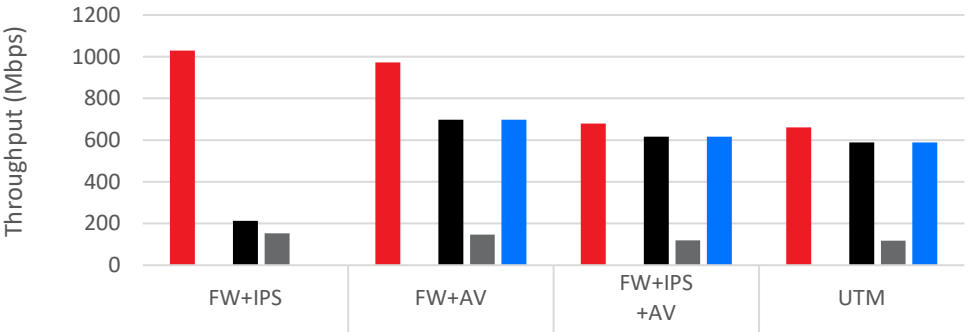


	FW	FW+IPS	FW+AV	FW+IPS +AV	UTM
Watchguard Firebox M270	2485	1821	2003	1285	1237
Cisco Meraki MX84	200	200	200	200	200
Fortinet FortiGate 100E	2706	2475	238	192	190
SonicWall NSA 2650	1748	1186	365	356	350
Sophos XG 210	3000	1205	712	658	646

Source: Miercom

Stateful HTTP traffic was generated using 6x1GbE ports of each DUT. Three ports acted as the client side, requested a 1 MB data file. The remaining three ports acted as the server side, responding with the file. The throughput from the egress ports was measured for a maximum line rate performance of 3 Gbps. The WatchGuard Firebox M270 maintained the best performance with FW+AV, FW+IPS+AV and UTM security features enabled. Its highest performance was observed for the firewall feature, where vendors were expected to see their best performance, reaching nearly 2.5 Gbps. Sophos achieved line rate performance for the FW only configuration. WatchGuard showed its next best performance for FW+AV, decreasing from its highest throughput by only 19 percent. In contrast, competitive performance fell by as much as 92 percent. With UTM threat protection enabled, WatchGuard achieved over 1.2 Gbps of throughput to outperform its best competitor by 47.8 percent.

Chart 3: Unified Threat Management Throughput for Stateful HTTPS Traffic



	FW+IPS	FW+AV	FW+IPS +AV	UTM
Watchguard Firebox M270	1030	972	680	661
Cisco Meraki MX84	N/A	N/A	N/A	N/A
Fortinet FortiGate 100E	213	698	616	589
SonicWall NSA 2650	153	147	120	118
Sophos XG 210	N/A	698	616	589

Source: Miercom

Stateful encrypted HTTPS traffic was generated using 6x1GbE ports of each DUT. As with the HTTP performance tests, the throughput from three egress ports was measured following the download of a 1 MB file from server to client. The maximum line rate was 3 Gbps. The Cisco Meraki MX84 does not support HTTPS, indicated by N/A. The Sophos XG 210 is unable to support encrypted traffic without the AV feature enabled, as reflected above. The WatchGuard Firebox M270 outperformed all vendors for every feature enabled with the firewall configuration. WatchGuard had the highest UTM performance at 661 Mbps – 11 percent higher than its best competitors and as much as 82 percent more than the SonicWall NSA 2650.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

In some cases, we had previously observed better performance throughput for some of the vendors' products tested, but the environment, including different firmware versions, test tools and traffic composition, was different.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and 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 in this report.

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.