#224128

July 2024

Commissioned by NetScaler

NetScaler VPX

Performance Benchmarking NetScaler VPX vs. F5 BIG-IP Virtual Edition

EXECUTIVE SUMMARY

Application delivery controllers (ADCs) are the unseen workhorses of the internet. Every back-end application that consists of two or more servers has an ADC of some type on the front end to optimize delivery to the application end user. ADCs are also called upon to handle security-oriented tasks. NetScaler VPX is a virtualized ADC designed to enhance the application end-user experience by providing high-performance traffic management coupled with low latency for delivering applications in hybrid cloud environments.

NetScaler commissioned Tolly to benchmark the performance of the NetScaler VPX virtualized ADC and compare it with the F5 BIG-IP Virtual Edition (VE). Tests were run in an Amazon Web Services (AWS) environment and included tests of ADCs running various combinations of traditional load balancing (LB), Policy (rewrite) processing, and application security (App Sec). Tests measured data throughput, CPU efficiency, and latency. For latency, tests measured P95 latency which measures the latency of the worst 5% of the flows.

NetScaler VPX outperformed F5 BIG-IP VE in all test scenarios, achieving lower (better) latency, better CPU efficiency, and higher throughput when running with similar CPU usage. See Figure 1.

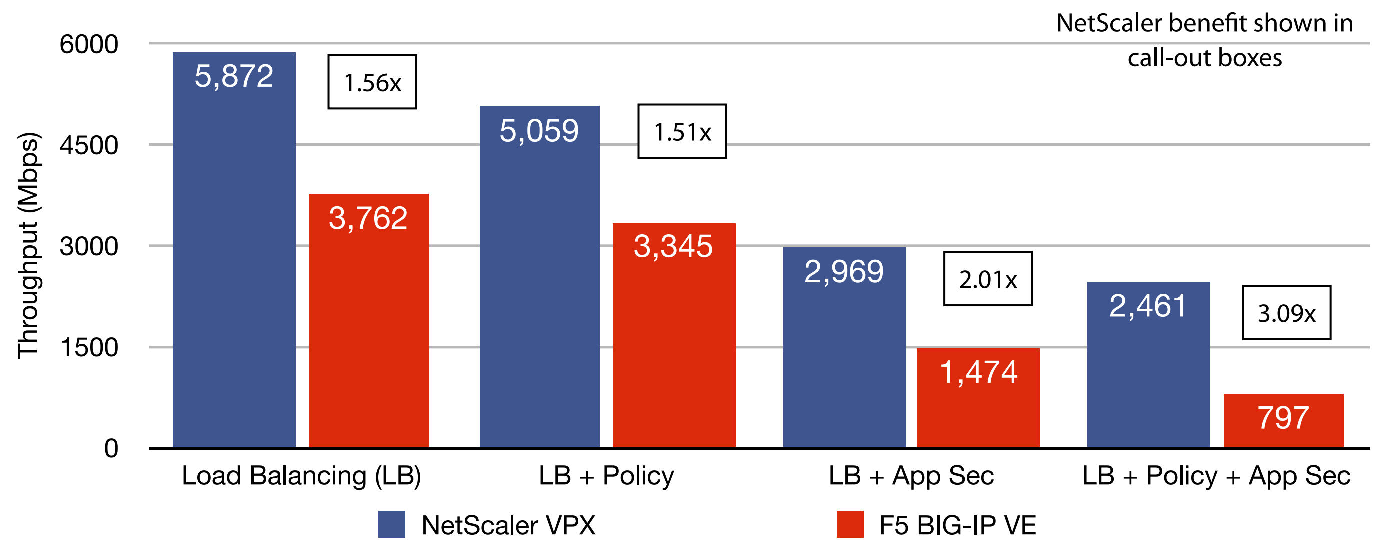
THE BOTTOM LINE

When NetScaler VPX was compared with F5 BIG-IP VE across all tests:

1. F5 performance declined significantly compared with NetScaler when carrying out multiple ADC tasks
2. NetScaler achieved up to 3x higher throughput for similar CPU usage
3. NetScaler demonstrated up to 64% more efficient use of CPU resources for a given throughput level
4. NetScaler induced up to 89% less latency per request
5. F5 latency rose dramatically with increasing user connections, showing just over 26x higher (worse) latency when compared to NetScaler

NetScaler VPX vs F5 BIG-IP VE: ADC Throughput for Similar CPU Usage (60%)

(Higher Result is Better)



Note: Load balancing used TLS 1.3. Policy scenario was a content rewriting policy. Load generated by Grafana k6.

Source: Tolly, June 2024

Figure 1

Key Takeaways

If any device can be said to be at the center of internet networking, it would be the ADC as it is positioned between the client and the web server, managing the traffic that constitutes the majority of internet activity.

The ADC's position in the client-server interaction makes it ideal for functions that go beyond traditional server load balancing. Increasingly, ADC administrators are leveraging the ADC's unique position to provide additional traffic policy and security enforcement.

Policy functions allow users to rewrite certain elements of the HTTPS headers to improve and personalize the user experience as well as to add further security.

App Sec functions provide for real-time scanning of web traffic for malicious traffic such as SQL injection attacks, cross-site scripting, and OS command injection.

While these functions benefit users, they add burdens to the ADC. If ADCs must make multiple "passes" at the traffic to run the additional functions, the CPU usage could go up while overall throughput goes down and latency degrades — meaning longer wait times. NetScaler notes that its single-pass architecture allows it to take on the additional functions without degrading performance.

Baseline tests were run first using only ADC load balancer functionality. Tests were then run enabling the following functionality: 1) LB + policy, 2) LB + App Sec, and 3) LB + Policy + App Sec for a total of four scenarios.

The goal was to highlight the performance difference between two of the largest ADC vendors in the industry by using four very common deployment scenarios, which makes these tests relevant to a very large audience.

Testing was carried out in the AWS cloud as a representative environment to test software ADC platforms, but the results are a measure of the software, itself, and translate to other environments outside of the cloud.

To provide useful comparisons, ADCs were benchmarked in scenarios where they had similar throughput and in scenarios where they had similar CPU usage. Finally, a test was run with varying numbers of simultaneous connections from 200 to 4,000 to reflect a relatively moderate workload typically encountered for a modern ADC.

There are 16 sets of throughput, CPU usage, and latency bars in this report. While the reader is encouraged to review each and every test, the results were consistent throughout. The NetScaler VPX delivered better results than the F5 BIG-IP VE in every variant of every test.

ADC Throughput for Similar CPU Usage

This test measured the throughput for each scenario when each device was loaded such that CPU usage was approximately 60%. See Figure 1 on Page 1.

NetScaler fared much better than F5 across all the tests. In tests of core load balancing, NetScaler throughput was 1.56x that of F5 at 5,872 Mbps compared with 3,762 Mbps.

Throughput, naturally, diminishes when additional security functions are enabled but these added functions impacted NetScaler less than they did F5.

NetScaler

NetScaler VPX

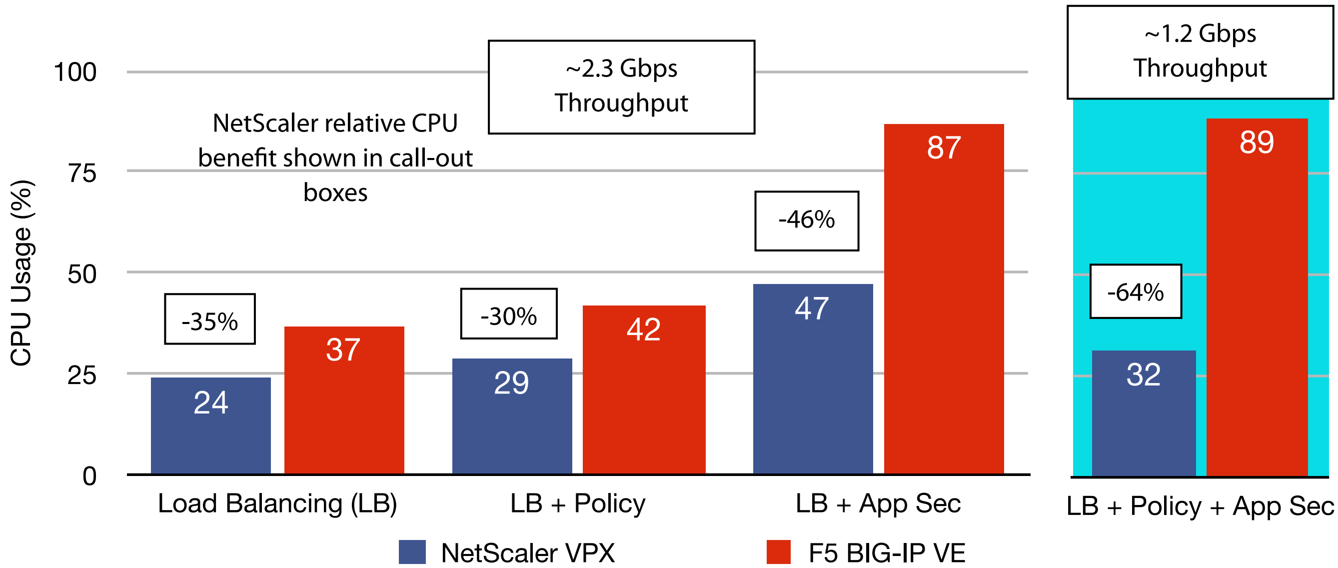
Software ADC Performance

Tolly Certified

Tested June 2024

With LB + policy, NetScaler throughput was 1.51x that of F5 at 5,059 Mbps compared with 3,345 Mbps. As additional functions were enabled, the performance differential between the two solutions widened.

With LB + App Sec, NetScaler throughput was 2.01x that of F5 at 2,969 Mbps compared with 1,474Mbps. With LB + policy + App Sec, NetScaler throughput was 3.09x that of F5 at 2,461 Mbps compared with 797 Mbps.



Note: Traffic generated by Grafana k6. For the LB + Policy + App Sec scenario, the F5 CPU hit 100% with a load higher than 1.2Gbps. Thus, the target throughput for that scenario was reduced for both systems to allow a fair comparison.

Source: Tolly, June 2024

Figure 2

ADC CPU Usage for Similar Throughput

This test measured the CPU usage for each scenario when the device throughput was approximately 2.3 Gbps. See Figure 2. This test had to be revamped for the LB + policy + App Sec scenario as F5 could not process 2.3 Gbps of throughput without exhausting CPU resource. So, for that test, the throughput level was throttled down to approximately 1.2 Gbps for both vendors to allow a fair comparison.

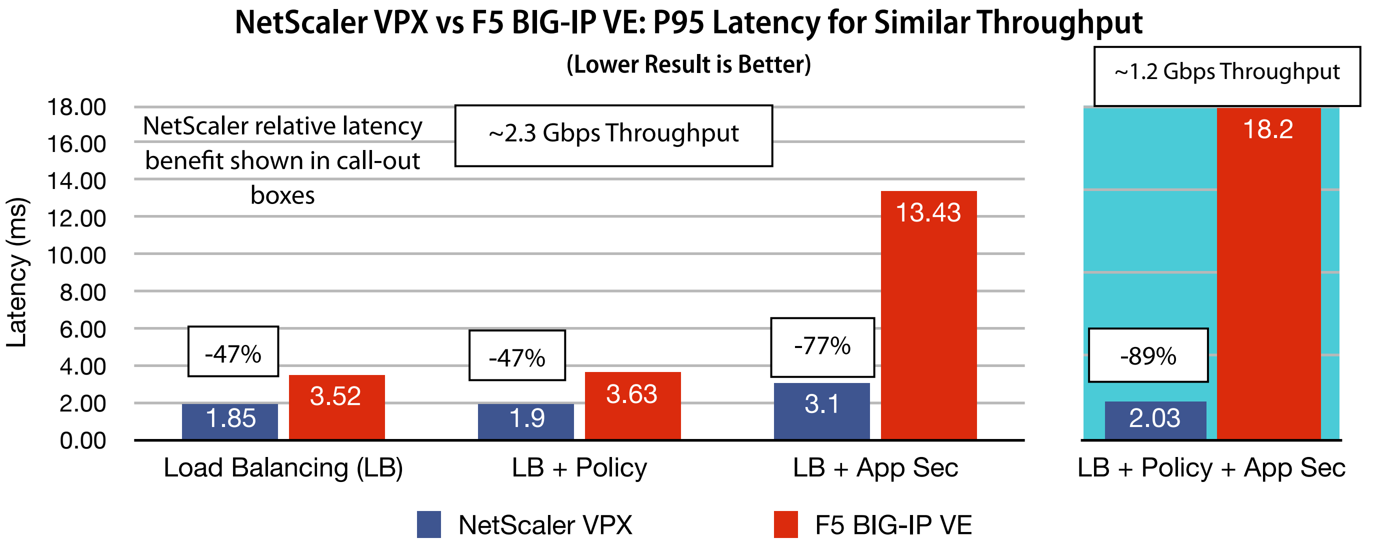
NetScaler fared much better than F5 across all the tests, showing lower CPU consumption across the board. In core load balancing tests, NetScaler CPU usage was 24%, which was 35% lower (better) than F5 CPU usage at 37%.

With LB + policy, NetScaler CPU was 30% lower than that of F5 at 29% compared with 42%. As additional functions were enabled, the performance differential, again, widened between the two solutions.

With LB + App Sec, NetScaler CPU was 46% lower than that of F5 at 47% compared with 87%.

As noted, for the LB + policy + App Sec test, the target throughput had to be scaled back to 1.2 Gbps to allow the F5 VE device to complete the test.

In these tests, NetScaler CPU was 64% lower than F5 at 32% compared with 89%.



Note: Traffic generated by Grafana k6. For the LB + Policy + App Sec scenario, the F5 CPU hit 100% with a load higher than 1.2Gbps. Thus, the target throughput for that scenario was reduced for both systems to make a fair comparison.

Source: Tolly, June 2024

Figure 3

P95 Latency for Similar Throughput

The last two tests measured latency, or delay. While measured in milliseconds for the ADC, delay accumulates from end-to-end and delay introduced by the ADC can only degrade the end-user session. Specifically, the type of latency trend measured was the duration between HTTP request and last byte of response. The initial DNS lookup, TCP connection establishment, and TLS handshake times were not included in the measurement.

This test measured P95 latency which, as noted above, is the latency of the worst 5% of the flows.

NetScaler notes that its architecture is "single pass." This means that it can process security and other functions simultaneously with the load balancing function. This being the case, the latency should remain low as additional security functions are enabled. Test results prove out NetScaler's claim.

This test was the same test as the prior test only now the measurements were of the latency rather than the CPU usage. See Figure 3.

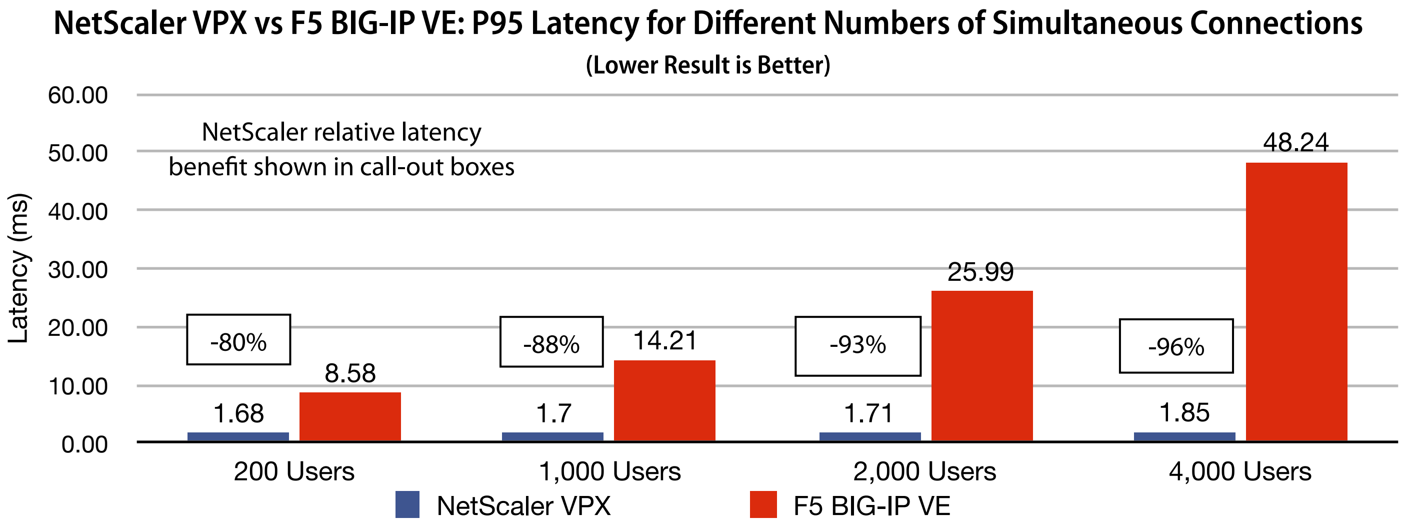
These results tracked the prior test. NetScaler's CPU usage was much more efficient and the induced latency was far lower than with the F5 device.

With LB alone, NetScaler P95 latency was 47% lower than that of F5 at 1.85ms compared with 3.52ms.

With LB + Policy, NetScaler latency was 47% lower than that of F5 at 1.90ms compared with 3.63ms.

With LB + App Sec, NetScaler latency was 77% lower than that of F5 at 3.1ms compared with 13.43ms.

With LB + Policy, NetScaler latency was 89% lower than that of F5 at 2.03ms compared with 18.2ms. 89% lower than that of F5 at 2.03ms compared with 18.2ms.



Note: Traffic generated by Grafana k6. Users are simulated by the test tool. 4,000 requests per second. Traffic load approximately 750Mbps.
Source: Tolly, June 2024 Figure 4

P95 Latency for Different Numbers of Simultaneous Connections

Simultaneous connections is another important aspect of scalability. As more simultaneous sessions are processed, each individual session can experience a degraded response time. P95 latency measurements can help identify the impact of session load on an ADC.

This test measured the latency at load levels from 200 to 4,000 simultaneous connections/users with LB + Policy + App Sec enabled. The differences between NetScaler and F5 were quite dramatic. See Figure 4.

At 200 users, NetScaler P95 latency was 80% lower than that of F5 at 1.68ms compared with 8.58ms.

As the connections scaled up to 4,000 users, the NetScaler latency was never higher than 1.85ms. By contrast, F5's latency for 1,000, 2,000, and 4,000 users was 14.21ms, 25.99ms, and 48.24ms, respectively. At 4,000 users, NetScaler's latency was 96% lower than that of F5 which means the response time would be faster and user experience would be far better.

Test Setup & Methodology

The focus of the test was to benchmark the performance of virtualized application delivery controllers. Benchmarking focused on measuring the network latency (delay), volumetric (data) throughput and CPU usage in traffic environments designed to model real-world conditions. See Tables 1-5 for details.

Comparable virtual appliances from Citrix Systems and F5 BIG-IP VE were tested in the Amazon Web Services (AWS) US cloud environment in June 2024 on m5.2xlarge instances with hyperthreading (HT) enabled. These provided for a base network throughput of 2.3Gbps with burst to 10Gbps.

The latest available releases at time of testing for both NetScaler and F5 were used.

ADC Configurations

Testing used one SSL content switching virtual server, forwarding the traffic to two HTTP virtual LB servers, based on matching string patterns in the HTTP request URL. Each HTTP virtual server has a pool of five backend web servers. Virtual Servers were configured on a single ADC appliance and tests were run with Local Traffic Policies and web application firewall (WAF) functions enabled or disabled on its content switching virtual server. Since almost all web traffic is now encrypted, all tests were run using encrypted sessions (detailed below) with HTTP 2.0 protocol on the front end and HTTP 1.1 on the back end.

For the App Sec scenario the F5 BIG-IP VE used the F5 Application Security Module (ASM).

Traffic Profiles

For all tests, web objects of various content types (text/html, image/png, svg, js) were used with an average size of 30 kB. The traffic profile was 80% "GET" and 20% “POST” with 50 Requests per L7 / User connection.

The real world traffic profile details were captured from public crawlers such as: https://crawler.ninja/files/top1mStats.txt, and https://httparchive.org/reports/state-of-the-web.

Test Procedure

Grafana k6 open source traffic generator was used to generate all traffic for the data throughput tests and measure the P95 latency of HTTP request duration. Grafana k6 was resident in the same VPC as the ADCs under test and simulated the client side of the connections. Tests were executed back-to-back, alternating NetScaler and F5 platforms to ensure consistent and fair testing (given cloud fluctuations and limitations). The test iteration duration was five minutes.

Test Details

Solutions Under Test (Cloud Instances)

Vendor	ADC	License	Version
NetScaler	NetScaler VPX	CNS_V10000_SERVER_PLT_Retail.lic	14.1-21.57 (Apr 23 2024)
F5	BIG-IP Virtual Edition (VE)	PAYG-Best Plus 10Gbps	17.1.1.3-0.0.5 (Apr 26 2024)

Table 1

Amazon Web Services EC2 Instance Information

Instance Size	vCPU	Physical Cores	Memory (GiB)	Network Bandwidth (Gbps)	Baseline Bandwidth (Mbps)	Notes
M5.2xlarge	8	4	32	10	2,300	HT enabled by default. SMT handling feature enabled on NetScaler, utilizing all available logical cores

Table 2

Test Variables

Scenario	Configuration
Load Balancing	TLS 1.3 + HTTP2.0 (Front End), HTTP 1.1 (Back End)
Policy	Content switching/Rewrite/Respond Rules (Responder 301 Redirect, Insert X-Forwarded-For Header, Delete Response Header (X-Powered-by), Insert Cookie header, Replace Request Header, Insert Response Header (Server Port), Insert header for specific cipher name match.)
App Sec	SQL injection, cross-site scripting, OS command injection inspection enabled
Note: “Check request headers” enabled for all tests.	

Table 3

Encryption Protocols

Encryption Protocol - Transport Level Security (TLS)	Notes
v1.3 TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384 and Elliptic Curve: X25519 used for testing

Table 4

Test Tools

Vendor	Solution	Function	Notes
Grafana	k6 v0.50.0	Traffic generation, latency and throughput measurement	Run on AWS m5n-8xlarge VM

Table 5

Source: Tolly, June 2024

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 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 by E-mail at sales@tolly.com, or by telephone at
+1 561.391.5610.

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

About NetScaler

NetScaler is the application delivery and security platform of choice for the world's largest companies. Thousands of organizations worldwide — and more than 90 percent of the Fortune 500 — rely on NetScaler for high-performance application delivery, comprehensive application and API security, and end-to-end observability.

NetScaler is a business unit of Cloud Software Group. https://www.netscaler.com/

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.

dj-n-wt-2024-07-03-VerM