

Title: Symantec Endpoint Protection 11v5	Document #: PD111809
Advisory Class: Performance Degradation	Impact: Severe
Date Published: 11/18/09	Date of Last Update: 11/18/09
<p><b>Performance Degradation Description</b></p> <p>PathView Cloud network performance system (<a href="http://www.apparentnetworks.com">www.apparentnetworks.com</a>) recently uncovered a parasitic network performance loss at the client side of the network path when the client was running Symantec Endpoint Protection (“SEP”) 11v5 with Network Threat Protection enabled. SEP 11v5 combines end point security, messaging security and backup/recovery into a single client-installed agent.</p> <p>The problem was uncovered when PathView Cloud’s diagnostic tests detected that test traffic was being clamped at regular intervals on the host system. Upon query, the host system identified a list of drivers which were considered potential sources of the problem. SEP 11v5 was among the suspects and therefore another test was run with SEP disabled. PathView Cloud then detected no problem. Upon additional testing, PathView Cloud results showed that severe packet loss and throughput disruption occurred at clients running SEP 11v5 as well. To confirm, Apparent Networks engineers performed independent tests offline—the results and methodology of those tests are outlined in this alert.</p> <p>While it’s expected that any additional layers of added-value management (be it security, data protection, monitoring, etc) can often exact some level of performance impact, the performance impact of SEP can be up to 70% of the available bandwidth. This means that SEP effectively caps TCP throughput to approximately 250 Mbps on a 1 GB network.</p>	
<p><b>Performance Results</b></p> <p>In general, at low to mid network throughput levels (namely at or around 100 Mbits/sec), SEP 11v5 had negligible adverse affects on either TCP or UDP performance. However, as the GigE network was pushed to higher throughputs, SEP did begin to impact throughput performance on both TPC and UDP and introduce significant packet loss on UDP.</p> <p>See table below:</p>	

Network Configuration and Test	Symantec Endpoint Protection 11v5 Base Configuration (Malware Only)	Symantec Endpoint Protection 11v5 with Network Threat Protection (NTP) Enabled
	Impact	Impact
1GBit TCP Throughput	None	Up to 70%
1GBit UDP Throughput	None	Up to 30%
1 GBit UDP Packet Loss	None	Up to 45%
100 MBit TCP Throughput	None	0%
100 MBit UDP Throughput	None	0%
100 MBit UDP Packet Loss	None	0%

Table 1A

**Products Tested**

Symantec Endpoint Protection 11v5

**Vendor Information, Solutions and Workarounds**

No known workaround is available, except to disable the Network Threat Protection.

## Test Description

To verify the problem, a simple Gigabit local area network was constructed consisting of three nodes connected via GigE switch. A Linux server, a WinXP Pro SP3 client running SEP 11v5, and an identical WinXP Pro SP3 client without SEP. In order to remove any possibility that the PathView Cloud measurement point was somehow affecting the results, it was turned off and an open source packet-flooding tool, iPerf (<http://en.wikipedia.org/wiki/Iperf>) was used to generate load and measure both TCP and UDP performance. See Appendix A for more details about testing configuration and methodology.

In particular, SEP effectively capped TCP throughput to approximately 250Mbps/sec on a 1Gbit network. This was validated by establishing baseline performance without SEP installed and comparing the results with SEP installed in Network Threat Protection (NTP) enabled and disabled. With SEP NTP disabled, performance returned to near baseline level. When re-enabled, the performance impact returned. In addition, at higher throughput levels, UDP performance was equally impacted and significant packet loss (up to 45%) was introduced.

## About PathView Cloud

PathView Cloud is a hosted network management tool that measures the performance of complete network paths from source to destination, including segments that pass through service providers' and carriers' networks. It enables IT teams and network managers to assess, troubleshoot and continuously monitor thousands of network paths simultaneously. A free version of the tool allowing users to monitor and test five network paths simultaneously is available at [www.apparentnetworks.com](http://www.apparentnetworks.com).

## About Apparent Networks

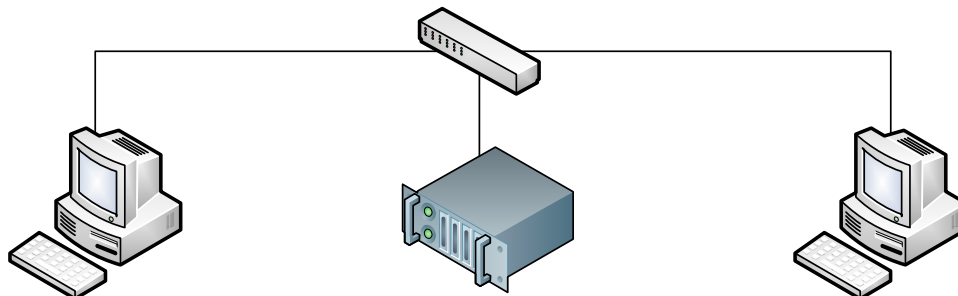
Apparent Networks is the only IT performance management provider that delivers the end-to-end service insight required for today's cloud applications. By experiencing network performance without affecting it, the company's patented path solutions (including PathView Cloud, PathView and AppCritical) assess network readiness, monitor service levels, and diagnose problems otherwise hidden from sight. Leading companies rely on Apparent Networks to assure application delivery and expand their service portfolios with confidence. For more information, visit [www.apparentnetworks.com](http://www.apparentnetworks.com).

## Disclaimer

The contents of this advisory are copyright (c) 2009 Apparent Networks Inc. and may be distributed freely as long as proper credit is given.

## Appendix - Testing Details

### Network and Hardware Configuration



	SEP Desktop	Clean Desktop	Server
Operating System	WinXP Pro SP3	WinXP Pro SP3	CentOS Linux v2.6
CPU	Intel Core 2 6300 1.86GHz	Intel Core 2 6300 1.86GHz	Intel Quad Core 2.33GHz
RAM	3GB	3GB	4GB
NIC	Broadcom NetXtreme 57xx	Broadcom NetXtreme 57xx	Broadcom NetXtreme II
NIC Driver	10.39.0.0	10.39.0.0	bnx2 v1.7.9-1
Network Speed	1000baseT	1000baseT	1000baseT

### Testing Methodology

The purpose of this testing was to determine if network performance was affected at various load rates. The well known packet flooding tool, iPerf, was selected as a reliable way to load down the network/NIC driver/OS networking stack to see how two identically configured machines except one with SEP 11v5 installed and one without performed side-by-side. Because certain parts of the SEP 11v5 installation remain on the client after de-installation, performance tests were run with Network Threat Protection disabled, SEP fully disabled, and SEP removed for comparison against baseline.

Before SEP 11v5 was installed on the "SEP" client machine, baseline tests were conducted on it and the "clean" client. Baseline measurements taken with Symantec Antivirus version 10.1.8.8000 installed.

Several tests were run, each at least twice to confirm results, more if results were highly variable in order to establish an average result. All iPerf tests ran for 30 seconds to let the network "settle". All one-way only tests were conducted from both server and from client to eliminate any "directional" variability in results.

## Raw Test Results

Tool	iPerf	iPerf	iPerf	iPerf	iPerf	iPerf	iPerf
Protocol	TCP	TCP	TCP	UDP	UDP	UDP	UDP
Load	Flood	Flood	Flood	Flood	Flood	100Mbps	100Mbps
Direction	2-way	1-way	1-way	1-way	1-way	1-way	1-way
Source	<i>Server</i>	<i>Server</i>	<i>Clean</i>	<i>Server</i>	<i>Clean</i>	<i>Server</i>	<i>Clean</i>

### SEP Baseline

Throughput	940/54.3	941	926	957	149	100	100	Mbps
Loss	N/A	N/A	N/A	0.0015%	0%	0%	0%	%
Jitter	N/A	N/A	N/A	0.14	1.007	2.452	0.179	ms

### Clean Baseline

Throughput	940/54.7	941	936	957	148	100	100	Mbps
Loss	N/A	N/A	N/A	0%	0%	0%	0%	%
Jitter	N/A	N/A	N/A	0.006	1.057	2.528	0.224	ms

### SEP Install SEP

Throughput	202/45.1	243	247	521	106	100	100	Mbps
Loss	N/A	N/A	N/A	45%	0%	0%	0%	%
Jitter	N/A	N/A	N/A	15.274	1.095	1.805	0.312	ms

### SEP Disable NTP

Throughput	911/85.3	939	874	957	128	100	100	Mbps
Loss	N/A	N/A	N/A	0%	0%	0%	0%	%
Jitter	N/A	N/A	N/A	0.049	1.06	2.345	0.248	ms

### SEP Disable SEP

Throughput	911/84.9	939	846	956	130	100	100	Mbps
Loss	N/A	N/A	N/A	0%	0%	0%	0%	%
Jitter	N/A	N/A	N/A	0.777	1.067	2.423	0.261	ms

### SEP Uninstall SEP

Throughput	939/57.5	941	924	957	164	100	99.9	Mbps
Loss	N/A	N/A	N/A	0%	0%	0%	0%	%
Jitter	N/A	N/A	N/A	0.024	0.689	2.457	0.375	ms