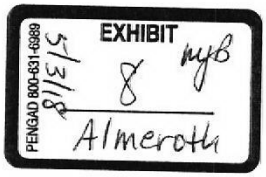
Ask Premier Field Engineering (PFE) Platforms

Why Are We Deprecating Network Performance Features (KB4014193)?

★★★★★

June 13, 2017 by BrandonWilson // 7 Comments



Hello, Michael C. Bazarewsky here again, with another short clarification post.

In February, we published Features that are removed or deprecated in Windows 10 Creators Update (KB 4014193). Someone I follow on Twitter noticed this part:

TCPChimney	X
IPsec task offload	X

The X's here indicate those features are deprecated. This occasionally comes up still on Twitter, with at least one person seeing this as a real issue...

But I was curious – what was the driving factor behind this deprecation? After all, you'd expect that if features improve performance reliably, and are in heavy use, we wouldn't deprecate them, right? Well, it turns out, by phrasing the question that way, I've walked you down the garden path a bit.

I reached out internally, and found out some interesting information that I'm not sure was particularly widely known, although you can see hints of it.

Before explaining why they are deprecated, though, I should explain what each of these features did, in theory, to explain why they were ever listed as features at all. After all, you can't really understand the implications of a change without understanding the original state, right?

First, let's talk about TCP Chimney, which is part of a larger concept known as TCP Offload Engine (TOE.) TCP Chimney moves part of basic TCP processing to a dedicated circuit on a network card. There are different levels of TOE implementation; TCP Chimney is a subset where the basic setup of a TCP connection is still handled by the host operating system stack, but once a connection is active, the encapsulation and de-encapsulation of data from the network stack into TCP packets over the connection is handled by the offload engine. The benefit is that it removes workload from the operating system and the host system processor cores. However, this benefit comes with some noticeable costs, as well:

- If there is a flaw in the TCP implementation in the network card, for example a security issue, you are potentially looking at a firmware update on the network card, or worse, you may be stuck with it, depending on the card implementation and the vendor's support policy for the network card.
- Under heavy network loads, performance may actually drop, because you're limited to the resources on the network card, which may be a bottleneck relative to a fast operating system stack with fast, available processor cores.
- The cost for all TCP connection offloading is fixed; there's no way for the operating system to optimize specific use cases. The feature assumes that the fixed cost will be offset by the CPU savings, thus there will be an overall improvement in performance. However, improvements in processor performance combined with what real-life TCP workloads look like suggest that, in 2017, ~99% of real-life connections will send enough data for the performance arithmetic to work out.
- The NIC code wasn't necessarily written with TCP in mind; thus, not all TCP features are implemented. For example, the TCP performance enhancement known as Selective Acknowledgement (RFC 2018, from 1996 [!!]), can't be used with TCP Chimney.

Windows first introduced TCP Chimney support as part of the Windows Server 2003 Scalable Networking Pack. As explained in KB 912222, even when first released, TCP Chimney had conflicts with other possible performance enhancements – so even at release, a customer saw the issue of not being able to leverage intelligence in the operating system network stack. Over time, as users called in with support cases, network card drivers were released to the Windows Update Catalog, and operating systems and servers moved forward, we found that several things were true:

1. Very few users actively used TCP Chimney support.
2. Very few network cards implemented the functionality.
3. Over time, less and less customers cared, and less and less NICs offered the ability.

4. In the Windows 7 / Windows Server 2008 R2 timeframe, we found that the number of customer support cases around this dropped to zero.
5. In Windows 8 / Windows Server 2012, we changed the operating system to disable this functionality by default. There was not a customer pushback on this.
6. The industry in general has decided this is not a necessary feature. For example, the Linux kernel has never implemented this capability, although some specific network card drivers did implement it, generally poorly. You do not need to take my word for this – the Wikipedia article on TCP Offload covers it sufficiently.

Thus, the end result of all of this is that the TCP Chimney deprecation in Windows 10 Creators Update is really not a new thing, because disabling it by default was a signal of the future direction. Furthermore, there are no current mainstream network cards that implement this feature, and customers are not reporting a need for this functionality. So, although deprecation of a feature is something customers generally need to be aware of and plan for, in this case, that's not a real life concern.

But what about the second deprecated feature, IPsec Task Offload? Well, this is another case of the concept of transferring computing responsibility from the host processor to the network card. However, this is not basic processing of TCP packets in this case. Instead, IPsec Task Offload, as the name implies, moves the encryption and decryption tasks for network data protected with IPsec to the network card. As you can imagine, this also requires a smarter network card, with more complicated firmware. Thus, all of the issues around updates and patches that were present for TCP Chimney are also present here. Further, because the whole point of IPsec is to secure network communications, security issues are arguably more critical to correct in this scenario.

Now, all of that may be okay if there was a sufficient benefit to customers. However, again based on customer support cases and driver support, we know that several things are true:

1. Processors and systems have gotten fast enough, and have added enough supporting processor instructions, that in most cases IPsec can be done quickly and efficiently on the host (and for that matter, more cost effectively), and improves faster than network card offloading technology. (This does, admittedly, leave the possibility of a workload that is so stressful on the host CPU that offloading could improve performance, although that's an uncommon edge case. That said, it's important to remember that "deprecated" does not mean "removed.")
2. Management of IPsec secrets can be complicated, and needing to interact with the network card to manage those adds another layer of complexity.
3. Conceptually, IPsec is a critical security feature in environments where it is used. All vulnerabilities that may exist are essentially critical vulnerabilities by definition; thus, the ability to quickly deploy changes is critical. As a major operating system vendor offering IPsec functionality, Microsoft has the dedicated security staff and deployment capability (with Windows Update) to make this happen.

4. Only one certified network card – an older Intel card – ever implemented this feature fully. No modern shipping mainstream network cards implement this functionality.
5. In the Windows 7 / Windows Server 2008 R2 timeframe, we found that the number of customer support cases around this dropped to zero.
6. Over time, the industry appears to be moving to TLS over IPsec for many use cases, such as VPN solutions, thus lowering the importance of IPsec workloads on Windows machines.

You may notice one of those points – the point around the number of support cases – is a duplicate from the list for TCP Chimney. This is not a coincidence. In both cases, it's clear from customer interaction that real-world impact of deprecation of these features will be near zero. And, as mentioned above, because deprecation is not the same as removal – the whole point of deprecation is to act as a customer warning point and allow reaction from the user community and ensure that we aren't missing something or breaking existing environments – there's always the chance for us to be proven wrong on this.

I hope you find this information helpful in understanding some of the thinking behind these features being deprecated (and, by extension, some of what we use in general for these decisions.)

Thanks!

p.s. What if you feel you are indeed impacted by these changes? In that case, that's what support channels are for. Open a support case, or, if you have Premier support, request a design change (DCR) through your account team. That's why we have those channels

p.p.s. special thanks to Daniel Havey, Mihai Peicu, Praveen Balasubramanian, Don Stanwyck, and Doug Stamper for technical review assistance and background information!

Tags

martin lucas Michael Hildebrand Networking O365 Performance PowerShell SBSL Security Server 2008 Server 2008 R2 Server 2012 Server 2012 R2 Tom Moser troubleshooting Windows Windows 7 Windows 8 Windows 8.1 Windows 10 windows server Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 windows server 2012 r2 Windows Server 2016 Windows Update WPA Xperf

Recent Posts

Delegate WMI Access to Domain Controllers April 30, 2018

Infrastructure + Security: Noteworthy News (April, 2018) April 27, 2018

Making Sense of Replication Schedules in PowerShell April 23, 2018

Nano Server 2018 Update April 16, 2018

Live Now on Server & Tools Blogs

Archives

April 2018 (6)
March 2018 (5)
February 2018 (5)
January 2018 (5)
December 2017 (6)
All of 2018 (21)
All of 2017 (54)
All of 2016 (45)
All of 2015 (63)
All of 2014 (66)
All of 2013 (90)
All of 2012 (64)
All of 2011 (4)

Tags #proudmicrosoftemployee features IP Michael Bazarewsky Networking Performance TCP TCPIP Windows Windows 10

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.