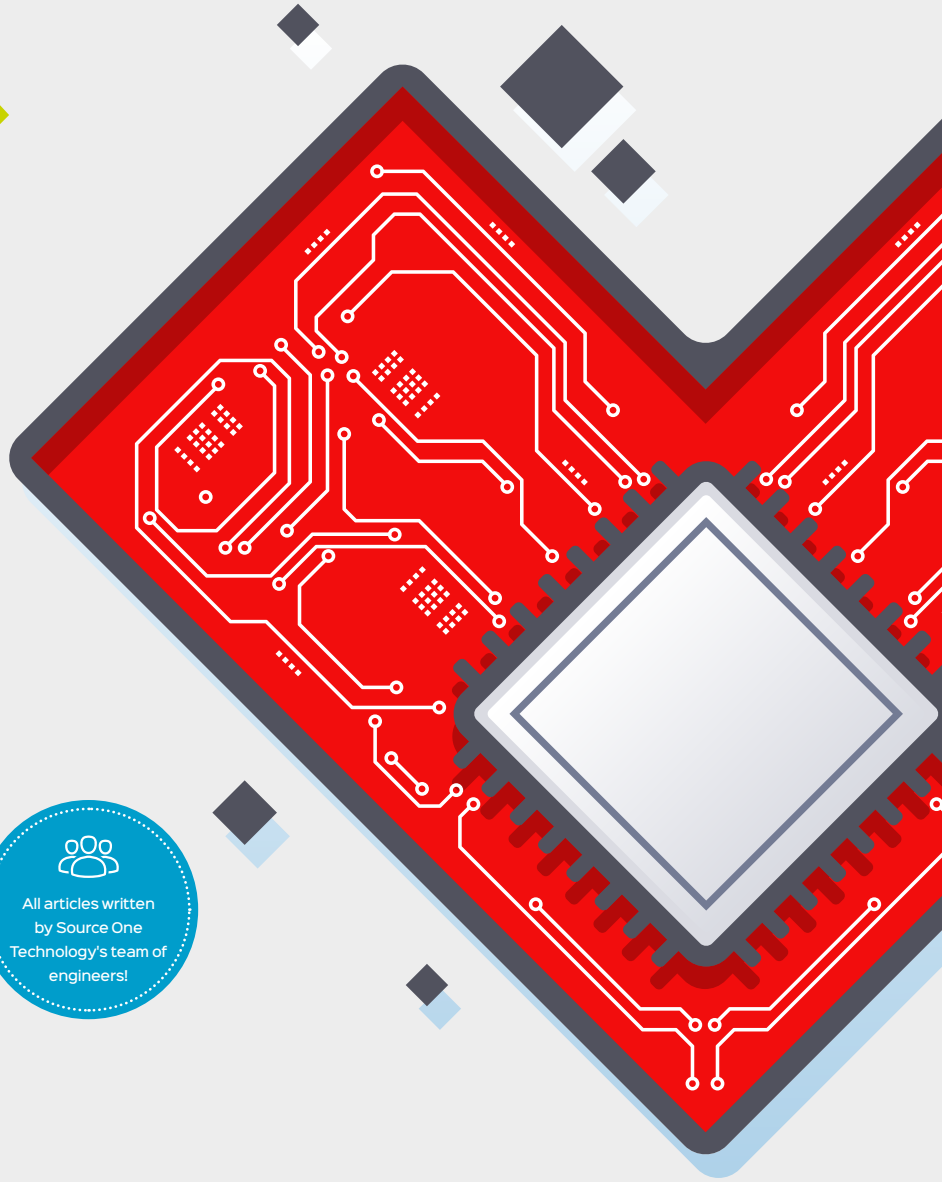
SPRING 2018

THE SOURCE

Hints, tips, tools and resources from real IT geeks.



Prevention is better than cure.

Keep your network in the best of health with our systems and security checklists.

IN THIS EDITION

- System Management
- Enabling Security Services
- Running Hyper-V
- Wi-Fi Connection Rates
- Auditing Active Directory
- ProjectSend

All articles written by Source One Technology's team of engineers!

Welcome!

Welcome to the Spring 2018 edition of The Source - hints, tips, tools, and resources for IT novices and experts alike.

In this edition, we show you how you keep your systems and network security in the best of health with a rundown of essential checks. We walk you through the process of running Hyper-V on 64-bit versions of Windows, and we compare the performance of WiFi standards. Finally, we do a bit of AD housekeeping and introduce you to ProjectSend.

I hope you find the magazine useful and if you have any other questions check out our blog, connect with us online or give us a call.

Sincerely, Jesse.

CONTENTS

Jesse Rink
OWNER, SOURCE ONE TECHNOLOGY.

An experienced network engineer, Jesse has been sharing his expertise and experience with schools and school districts in Wisconsin for over 18 years.

Source One Technology provides IT support to businesses, schools and nonprofits across Southeastern Wisconsin.

ALL SYSTEMS GO

Systems management checklists & health checks.

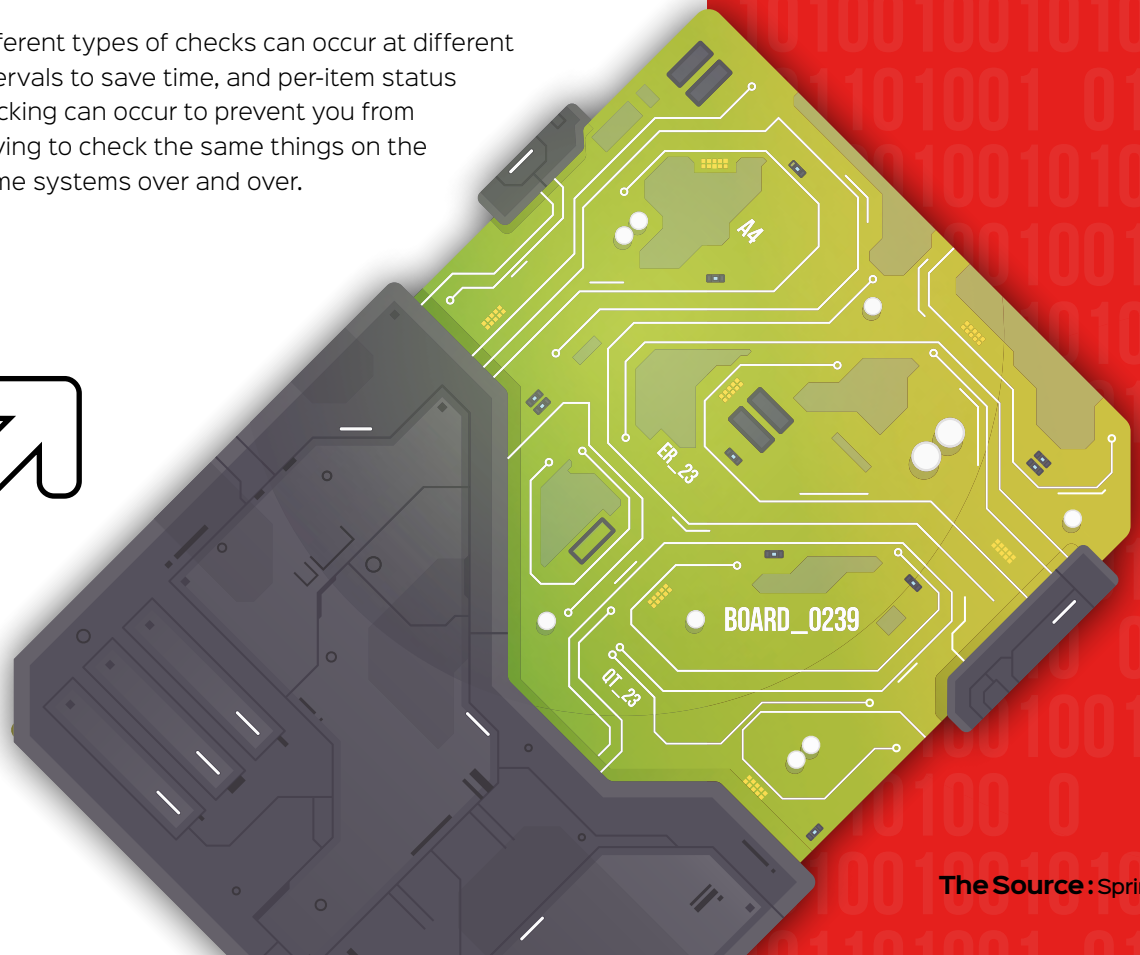
Are all of your servers monitored, backed up, replicated, patched, and protected by your host-based anti-malware solution? When was the last time your hypervisor HA, firewall HA, ISP, and power backup failover systems were tested to confirm they worked as expected?

There exist a variety of configuration and failover mechanisms that are both simultaneously difficult to monitor and vital to the ability of the organization to react to unexpected or unusual circumstances.

Without highly systematized processes and automated deployment mechanisms, which are out of reach to smaller organizations, many organizations find that they are failing to adequately protect some of their systems fully because their product consoles are designed only to let you know about failures for systems you remembered to add to the product.

One solution for smaller organizations is to implement recurring periodic checks to ensure that changes to the environment made by various team members (or external actors) have all been incorporated into a plan that looks for things that might have been missed.

Different types of checks can occur at different intervals to save time, and per-item status tracking can occur to prevent you from having to check the same things on the same systems over and over.



Source One TECHNOLOGY

→ CHECKLIST

For an example of a sample checklist that has a separate sheet for tracking the status of individual items, please see:

http://bit.do/S1THealthCheck.

Enabling UTM and NGFW security services.

Are you blocking access to known botnets? Are you preventing people from simply bypassing policies by using proxies? Are you preventing someone from submitting 10,000 logon requests to your Domain Controller in a lockout attack?

By default, network security appliances performing Unified Threat Management (UTM) or Next Generation Firewall (NGFW) functions are not performing any inspection except for blocking traffic that hasn't been explicitly allowed.

If you have valid subscriptions and are not currently experiencing performance problems you should ensure you slowly enable and apply the following features to most of your traffic, **in descending order**, monitoring performance as each feature is enabled.

01

Intrusion Prevention (vulnerabilities and attacks)

Set to block Medium and above threat to any traffic to/from any.

02

SSL/TLS Decryption

Over 70% of web traffic is now encrypted, and many of the following security services simply cannot work without full deep packet inspection. Apply, minimally, to any traffic to WAN.

03

Anti-malware/Gateway Anti-virus and Anti-spyware

Set to scan all available protocols and inspect all traffic.

04

Botnet/C&C and Geo-IP

Apply to any traffic to/from WAN, blocking inbound countries for nearly all countries and outbound for all countries for which no known use case exists.

05

Content Filtering/URL Filtering and Application Control

Set to block proxies, malware, peer-to-peer, and, if feasible, unrated sites, for any traffic to/from WAN.

06

Sandboxing

Configure executables and archives for sandbox analysis.

VENDOR-SPECIFIC GUIDES

- **FortiGate:** Security Fabric Audit
- **FortiGate:** Security Profiles
- **SonicWALL**
- **Palo Alto Networks**

Click vendor to read the guide.

VIRTUALIZATION

Running Hyper-V on Windows 8 or 10.

Many server administrators are aware of Hyper-V virtualization that is available on Windows Server, but did you know it's available as a feature in 64-bit versions of Windows 8 or 10 Pro, Enterprise or Education editions as well?

To run the hypervisor platform, your system must both have robust specs and support virtualization technologies (many recent systems do). Check the Performance tab of Task Manager to see if Virtualization is enabled. If it is, you're good to go! If it's disabled, then just reboot, enter your BIOS or UEFI, and enable the option called "*Intel Virtualization*" or "*Intel VT-x*". If you switched from Blue to Red, you would be looking for an option called "*AMD-v*".

Finally, to enable Hyper-V in the operating system,

- Boot back into Windows
- Open Control Panel
- Open Programs and Features
- Select Turn Windows Features on or off
- Enable the Hyper-V Platform and Management Tools
- Complete the installation and reboot your system

Whether you want to run a small test or lab environment on your system, or simply learn the platform, you can now take advantage of Hyper-V functionality available to enterprise customers* on your laptop or desktop!

*Excludes RemoteFX, replicas and live migrations. Batteries not included.

Wi-Fi connection rates.

Those of us who implement, manage or maintain wireless infrastructure are aware of the multitude of Wi-Fi networking standards. It's easy to think back and *re-associate* (see what we did there?) 802.11g with 54Mbps. But what immediately pops into your mind when you think of n, ac or the next big thing?

802.11n changed the Wi-Fi landscape with dual-band radios, MIMO (multiple antennas and spatial streams) and beamforming. These technologies, combined with signal modulation, strength, and environmental factors result in connection rates between 72Mbps and 600Mbps.

However, real-world throughput and transfer rates are usually much lower than connection rates. This is due to additional factors including overhead, interference, the number of clients and at which speed those clients are connected.

We averaged and condensed real-world throughput and typical transfer rates to what we typically see in industry:

802.11n at a glance.

Antennas / Streams	1 x 1	2 x 2	3 x 3	4 x 4
2.4GHz @ 20Mhz	72Mbps	-	-	-
5GHz @ 20MHz	72Mbps	144Mbps	216Mbps	288Mbps
5GHz @ 40MHz	150Mbps	300Mbps	450Mbps	600Mbps
Real-World	30-50Mbps	60-70Mbps	80-150Mbps	150Mbps
Typical Transfer	4-6MB/s	7-9MB/s	10-19MB/s	19MB/s

Though 802.11n networks remain common in 2018, 802.11ac takes performance to another level. It builds on MIMO by introducing SU-MIMO (Wave 1) and MU-MIMO (Wave 2). SU (to one extent) and MU-MIMO allows multiple compatible clients to simultaneously communicate with an access point, increasing potential REAL-WORLD throughput by minimizing the sharing of (limited) airtime with other clients.

Connection rates have been bumped up to 200Mbps – 1.7Gbps (the spec has a theoretical upper limit in excess of 3Gbps, but this is typically found only in perfect laboratory conditions).

802.11ac at a glance.

Antennas / Streams	1 x 1	2 x 2	3 x 3	4 x 4
40Mhz	200Mbps	400Mbps	600Mbps	800Mbps
80MHz	433Mbps	866Mbps	1333Mbps	1732Mbps
160MHz	866Mbps	1732Mbps	2301Mbps	3468Mbps
Real-World	80-170Mbps	160-350Mbps	200-500Mbps	300-700Mbps
Typical Transfer	10-21MB/s	20-44MB/s	25-63MB/s	38-88MB/s

Wave 2 introduces support for 160MHz channels, but we generally don't recommend pushing beyond 80MHz (and sometimes 40MHz) unless you're in a residential or low-density deployment environment.

While 802.11ac performance is nothing short of amazing, keep your eye on 802.11ax for 2019, which promises 4x the performance of 802.11ac!

Company News

- We completed our move to offices in Brookfield, WI. and are adding more network engineers to our team.
- *On the blog:* Run your Windows apps on Chromebook.
- *Coming soon:* A special network security edition of The Source magazine for schools which will be out in June!

Auditing Active Directory changes.

There's one place in just about every network that quietly does its job and doesn't get a ton of attention. Our good old friend Active Directory (AD) manages each and every bit of who can access what and how.

Over time, users are added to groups and rarely removed. Also, users are often granted “temporary” upgrades rights and privileges, but the “temporary” is forgotten about after some time. To prevent things from getting out of hand, we should periodically review Active Directory permissions from time to time.

Tools for auditing Active Directory are extremely useful not only for keeping track of who has access to what, but most importantly, what has changed.

When things stop working, every technician’s first response is usually "What's changed?". With tools monitoring AD, we know instantly who's been added to what groups, what GPO was just edited, what accounts are expired, or even simply when a password was last changed. Having that information lets your IT department be more proactive instead of reactive!

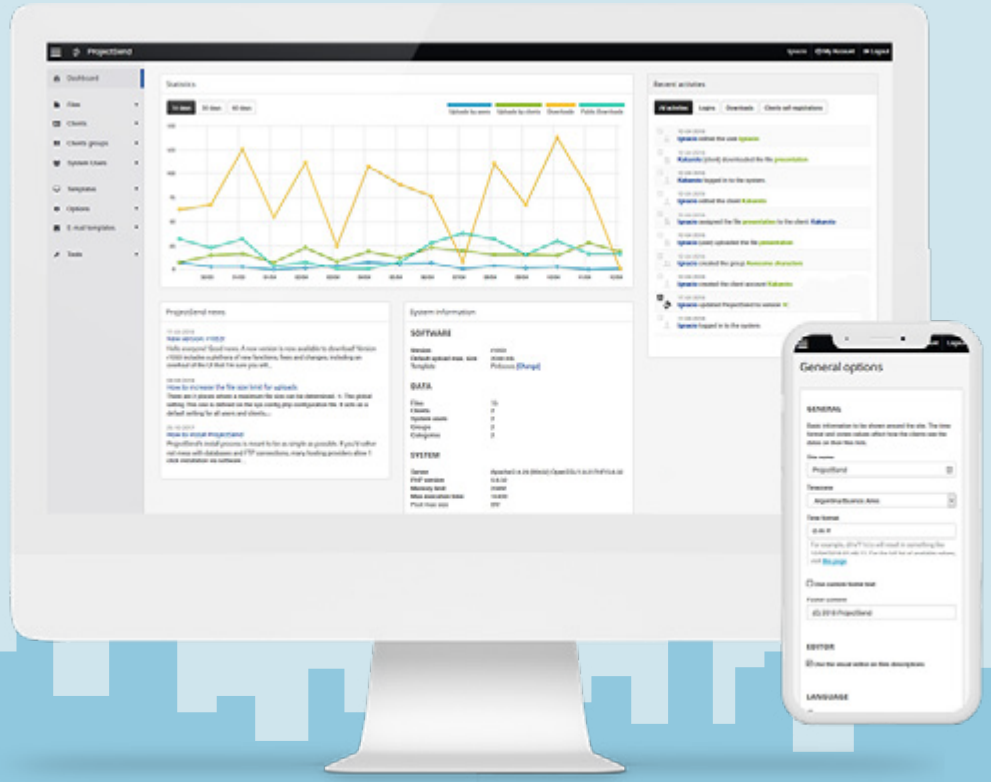
Think about having a quick report available that says, "Michael can't log in because his password just expired" instead of having him get frustrated and storming up to your office and complaining that the network is broken (again). Or have you ever wondered, “How on earth did <insert-user-here> get added to the Domain Admins group and when did that happen?”. Wouldn’t it have been helpful to receive an email notification when users are added/removed from AD security groups?

Active Directory auditing tools are extremely valuable to have. Yes, there might be a small cost associated with the really good auditing tools, but in the long run, they easily pay for themselves.

OPEN SOURCE

SIGNED, SEALED, DELIVERED.

ProjectSend is for organizations that want to have a user-friendly secure way to share files between their customers and maintain complete visibility on all transactions that have taken place.



Administrators and customers accounts can download or upload files and can opt-in for email alerts when file changes are detected.

ProjectSend is a self-hosted web application you can run on your on-premise server or virtual private server.

- Free / Open Source software - donations welcomed
- Large file transfer support
- File change email notifications
- Optional self-registration and approval features
- Auto-expiration of uploaded files
- Detailed access logs and statistics of all transactions
- Fully customizable user interface / brandable

There are hundreds of file sharing services out there, but if you require more control of where your data exists, then be sure to try out ProjectSend!

Website:
PROJECTSEND.ORG

Demo:
SOFTACULOUS.COM/DEMOS/PROJECTSEND

LOVE FREE?

If you like getting impartial advice, practical tips, and pointers to great free software, then we've got even more for you!

CONNECT

Read the latest from our engineers or ask us a question whenever you need advice.


sourceonetechnology.com/blog


@sourceone_wi


linkedin.com/company/source-one-technology-inc

I approached Source One Technology last year, as I was unhappy with our service provider. We have a school that depends on computers for education, testing, and administration, and Source One Technology has solved all of our issues in the first year of doing business with them.

Patti Penkalski
BUSINESS MANAGER
ST. GREGORY THE GREAT

See what our customers are saying about us
sourceonetechnology.com/testimonials

Source One TECHNOLOGY

Call us on (262) 993 2231 or visit www.sourceonetechnology.com.
333 Bishops Way, Suite 120, Brookfield, WI 53005.