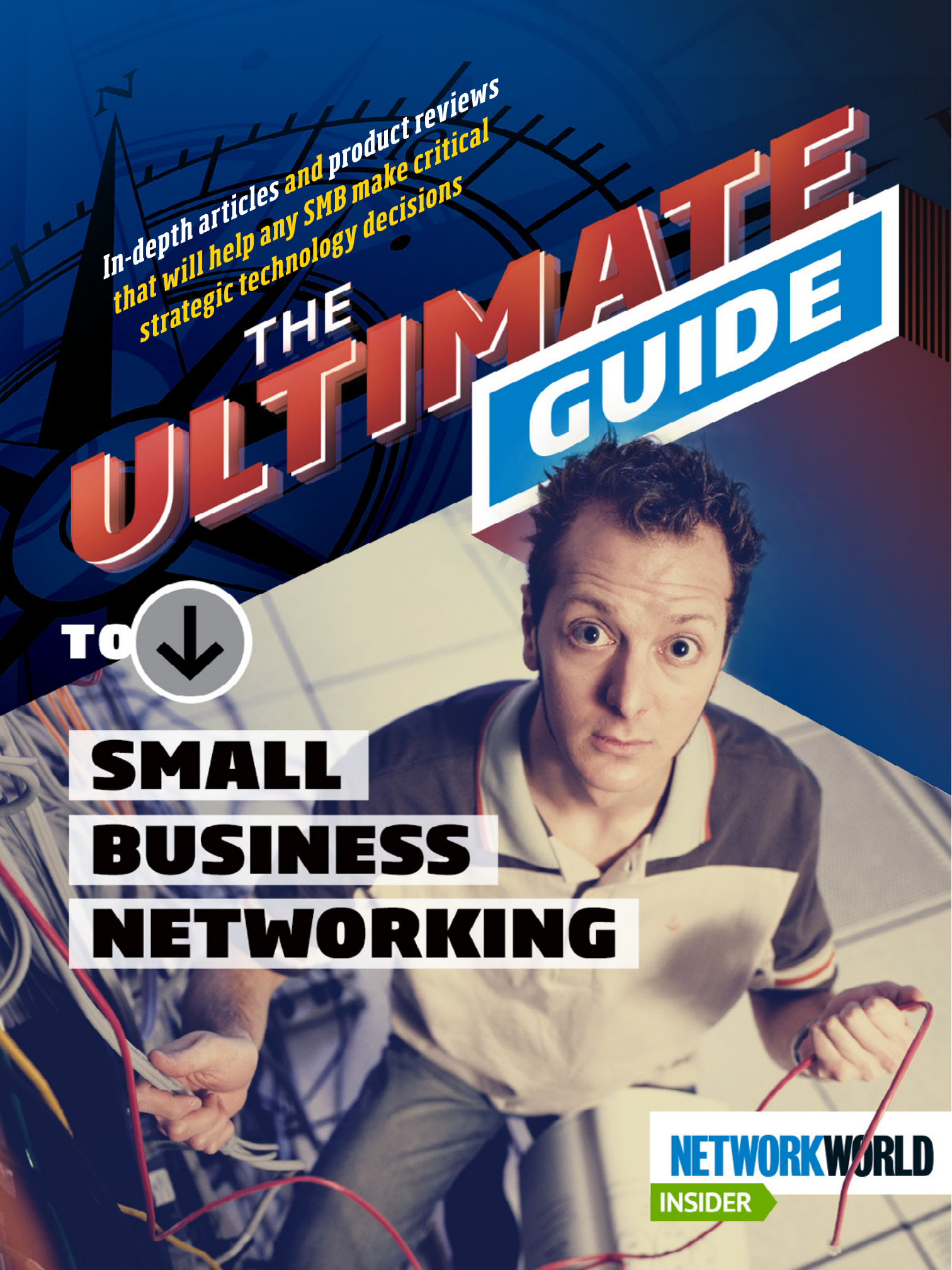
In-depth articles and product reviews that will help any SMB make critical strategic technology decisions

THE ULTIMATE GUIDE

TO

SMALL BUSINESS NETWORKING



NETWORKWORLD INSIDER

INSIDE

THE ULTIMATE GUIDE

SMALL BUSINESS NETWORKING

Small businesses have two significant challenges when it comes to building a network. First, a small business might not have the in-house expertise in areas like networking, security, storage and Wi-Fi. Second, an SMB might not have the budget to spend big on networking gear. However, building an effective network infrastructure is critical for an SMB in order to compete with larger competitors who may have better name recognition and bigger marketing budgets. Small businesses need to deploy their tech resources wisely in order to create a business that's agile, flexible, fast and efficient. In this PDF we compiled six in-depth articles and product reviews that will help any SMB make critical strategic technology decisions, as well as buying decisions in key areas like security, Wi-Fi and network attached storage (NAS.)

THE ULTIMATE GUIDE

BY ERIC GEIER

BEST VPN ROUTERS FOR SMALL BUSINESS

WE looked at six VPN routers designed for small businesses, ranging from the popular Cisco brand to lesser-known names like DrayTek and UTT Technologies. We setup and evaluated each to determine how they compare in regards to price, features, and user-friendliness.

When choosing a VPN router, you want to pick one that supports the VPN protocol of your choice. If you're look for an IPSec VPN, consider those that provide a way to simplify the configuration, such as the Cisco, Linksys or Netgear units. If you're looking for a wide variety of VPN options, consider D-Link.

If you're looking for an inexpensive option, consider UTT Technologies. And if you're looking for unique features, consider the DrayTek unit, or their other models with integrated Wi-Fi, fiber, or VoIP support.

Cisco RV325

The Cisco RV325 is a Dual Gigabit WAN VPN Router with a price of $468, but

NetResults

	Cisco RV325	D-Link DSR-250	DrayTek Vigor2925	Linksys LRT224	Netgear FVS336G	UTT Technologies HiPER 518
Price	$468	$189	$288	$249	$425	$69
Pros	• Plenty of switch ports • Supports Cisco Easy VPN	• Many VPN options • USB file and printer sharing	• Feature-rich • Unique functionality	• EasyLink VPN simplifies IPSec • High throughput ratings	• VPN client program simplifies IPSec • Great on-screen help	• Inexpensive • PPPoE server and web authentication
Cons	• Only site-to-site option is IPSec • USB ports don't support file or printer sharing	• Lacks second WAN port • GUI could be better	• Lacking on-screen help • GUI could be better	• No SSL VPN • Only 5 simultaneous PPTP tunnels	• Only site-to-site option is IPSec • GUI could be better	• No VLAN support • Low IPSec throughput rating

it can be found online for less than $300. It is the top model from Cisco's small business RV VPN router series. A couple of the lower models have Wi-Fi included, although this model doesn't.

This Cisco unit supports up to 50 IPSec tunnels, either site-to-site or client-to-site connections, with an advertised IPSec throughput of around 100Mbps. The PPTP and SSL VPN servers both support up to 10 simultaneous client-to-site tunnels each.

In the box, you'll find an Ethernet cable, power adapter, quick start guide, and a CD with full documentation. Also included are L brackets for mounting in a standard 19-inch rack.

The unit measures about 9 ½ inches wide, 2 inches high, and 7 inches deep. The outer case is mostly gray metal. On the back side of the unit is the power input and switch. On the bottom are pre-applied non-slick pads for desk or shelf placement along with holes for wall mounting.

On the front of the unit, you find the status lights, 14 switch ports, two WAN ports, and reset button. You also find one USB port on the front and a second on the side, both of which can be used for either 3G Internet failover or maintenance usage.

After logging into the web GUI, you're met with the Getting Started page with shortcuts to run the setup wizard, set initial settings,

and other common pages. The basic setup wizard helps you configure the WAN ports and the access rule wizard helps you add firewall rules. The main menu for the GUI is on the left, categorized into a couple expandable lists. From any page, you can click the Help shortcut in the upper-right corner, which brings up a description of the settings on that particular page.

While going through the VPN settings, we found the unit supports the Cisco Easy VPN solution that simplifies the configuration of remote VPN users. However, we found the only site-to-site VPN option is IPSec. It would be nice to see other site-to-site options, as IPSec is never the simplest to configure.

After evaluating the unit, we found the GUI to be simple and straightforward. This is a solid unit with the most common VPN router features and functionality.

D-Link DSR-250

The D-Link DSR-250 is an eight-port Gigabit VPN router with a list price of $189.99, but can be found online for around $115. It is one of several models in the DSR line. Like the other models, there is a wireless version of this unit that adds 802.11n Wi-Fi.

This D-Link model supports six VPN types. It supports up to 25 simultaneous site-to-site or client-to-site IPSec connections with a max throughput of around 50Mbps. The SSL VPN supports up to 5 tunnels. Also included is a server and client for both PPTP and L2TP VPN connections, supporting up to 25 tunnels. An OpenVPN server and client supports up to 5 tunnels. Lastly, the unit supports up to 10 GRE tunnels, enabling remote networks to receive the LAN broadcast traffic.

Along with the DSR-250 unit, in the box you'll find a power adapter, Ethernet cable, and Ethernet-to-serial console cable. You won't find any install guide like most other vendors include. However, the CD includes PDFs of the install guide and full manual.

The unit measures about 7½ inches wide, 1½ inches high, and 5 inches deep. The outer case is all black finished metal with the vendor name embossed on the top.

On the front of the unit, you'll find a USB 2.0 port for 3G Internet failover, file or printer sharing, or maintenance usage. Plus there are eight Gigabit switch ports, a Gigabit WAN port, and an Ethernet port for console access. There's a simple power light and then activity lights for the ports. There are no wall mounting holes, nor mounting bracket included; just the small non-slick pads you can apply to the bottom of the unit if you're placing it on a table or shelf.

After logging into the web GUI, you're met with the status dashboard, sporting a couple graphs of traffic and resource stats.

You can optionally click the Wizard link in the upper-right corner of the GUI to run one of the

wizards to configure different settings. Hovering over the menu categories on the top of the GUI pops up a listing of all the setting pages in that particular category. In the upper-right corner of each setting page, you see a question mark button, which you can click to bring up the help on that particular page.

The GUI is attractive and straightforward, but some improvements could make it even more user-friendly. For instance, you must manually input all of the IP and DHCP settings for the subnets of VLANs you add. Many routers automate or pre-configure most of these settings for you when adding VLANs.

In addition to the typical VPN router features, this unit supports Intel AMT to enable the management of computers when powered off or when lacking a hard drive or OS. It also supports dynamic web content filtering, but requires purchasing a subscription at approximately $60 per year.

Overall, this D-Link unit is a feature-rich router. It supports a wide variety of VPN options, offers USB file and printer sharing, and supports dynamic web content filtering. Our gripe about the GUI is minor.

DrayTek Vigor2925

The DrayTek Vigor2925, priced at $288, is a dual-WAN Gigabit VPN router offering five switch ports. It is one of many models provided by DrayTek, each of which offer a few different editions to support varying Wi-Fi standards, fiber connections, and VoIP support. We choose to include its basic edition, which lacks those extra functionalities.

This unit supports up to 50 concurrent VPN tunnels via site-to-site or client-to-site with IPSec, PPTP, or L2TP. IPSec tunnels are rating at 50Mbps for throughput. The SSL VPN server supports up to 25 client-to-site tunnels.

In the box along with the unit, you'll find a quick start guide, CD with full documentation, Ethernet cable, and a power adapter.

Its black plastic body measures about 9½ inches wide, 1½ inches high, and 6½ inches deep. On the front, you'll find all the status lights and ports, except for the power input and switch on the back. On the front-left is the factory reset button, status lights, and two USB 2.0 ports for 3G Internet failover, file sharing via SMB or FTP, or printer sharing. Then there's two WAN ports and also five switch ports. On the bottom of the unit are non-slip pads and also four holes for optional wall mounting.

After plugging in the unit, we didn't get Internet access right away. Unlike most routers, the WAN connections aren't set to get a dynamic IP by default. You have to go into the web GUI to enable that. If you have a static IP, this doesn't

matter, but if you have a dynamic IP, it's a little inconvenient.

After logging into the web GUI, you're taken to the dashboard page showing the main stats along with an image representing the front of the router and it's status lights. You aren't prompted by any wizards, but they do offer a few, accessible from the top portion of the main menu on the left.

The collapsible main menu on the left is organized into categories that display related pages when you click on them. Some pages also have multiple tabs you can click through. Some pages have an info or help button you can click to get more info, but it is not consistent throughout the GUI. The GUI could also use some more organization and sprucing up to make it more attractive and user-friendly.

We found this DrayTek unit to be feature-rich, supporting all the major VPN solutions except OpenVPN. In addition to the features typically found in VPN routers, it includes dynamic web filtering, central VPN and wireless access point management, and FTP access (in addition to SMB) for the USB-based file sharing. It also has some unique functionality as well, such as support for temperature monitoring via a USB sensor.

Linksys LRT224

The Linksys LRT224 is a Gigabit four-port dual-WAN VPN router with a list price of $249.99, but is available online for around $175. It is one of the two business-class VPN routers they offer. The other model (LRT214) is very similar, but lacks the dual WAN ports along with WAN load balancing and failover that the LRT224 offers.

This Linksys unit supports up to 45 IPSec tunnels, either site-to-site or client-to-site connections, which they claim has a max throughput of 110Mbps —the highest among the routers we reviewed. The PPTP-based VPN server supports up to five concurrent users. The OpenVPN server supports up to five incoming client-to-site tunnels and the OpenVPN client allows you to perform a site-to-site connection.

The unit also includes its new EasyLink VPN feature, designed to simplify site-to-site IPSec tunnels, which thus far is only supported by this and the other LRT model. The server supports up to five simultaneous incoming connections via a single username and password and then the client supports one outbound connection.

Inside the box you'll find a power adapter, Ethernet cable, quick installation guide, and a CD with the full documentation in addition to the unit itself.

The unit measures about 5 inches wide, 1½

inches high, and 7½ inches deep. It's metal case sports Linksys's black and blue color scheme. The unit can be sat down for desktop/shelf placement or can be mounted on the wall using the two built-in mounting holes on the bottom/back of the unit.

On the front top area are the LED status lights for the system, diagnostics, WAN, WAN/DMZ, VPN, and the four switch ports. On the back side are the Gigabit Ethernet ports: four switch ports, WAN port, and a WAN/DMZ port.

After logging into web-based admin interface, you're met with the System Status page on their tabbed GUI. There you can review the main stats and optionally launch their Setup Wizard, which prompts you to set the WAN, LAN, time, and password settings. You can also access the Setup Wizard by clicking the Quick Start tab.

The majority of settings are accessible via the Configuration tab, which contains sub-tabs categorized on the menu to the left of the page. The Maintenance tab also contains a couple sub-tabs of tools. The last tab, called Support, is just a simple page offering shortcuts to Linksys's main business product and support pages. It would be more useful if these led directly to this particular model's product and support pages, however.

On the top of the web GUI you'll find the Help link, which conveniently brings up the documentation for settings of the page you're currently on. This pops up a browser window, but the content comes from the router, thus it's accessible off-line and is printer friendly as well. You can also browse and search through the help content too. Also handy on the top of the web GUI is the Page Width selector, allowing you to easily change between page sizes.

This Linksys unit seems to be a solid choice for those wanting IPSec VPN, as they advertise the highest throughout among the routers in this review and offer simplified configuration. However keep in mind, it provides no browser-based SSL VPN functionality and the max amount of PPTP VPN tunnels is only five.

Netgear FVS336G

The Netgear FVS336G is a dual-WAN VPN server that costs $425, but can be found online for around $230. It is Netgear's middle-of-the-road option when compared to its other VPN routers. The model under this offers only one WAN connection, supports less VPN tunnels, and lacks SSL VPN, but a wireless model is also offered. The model above this one supports up to four WAN connections, provides higher throughput, and supports more VPN tunnels.

This Netgear model supports up to 25 IPSec site-to-site or client-to-site tunnels, with an advertised max throughout of 78Mbps. The SSL VPN server supports up to 10 tunnels and the PPTP and

L2TP VPN servers support up to 25 users.

Along with the unit, in the box you'll find an installation guide, CD with documentation and VPN client software, Ethernet cable, power adapter, and non-slip rubber feet for table or shelf usage.

The unit's all metal casing measures about 10 inches wide, 1 ½ inches high, and 7 inches deep. On the front of the unit are the status LEDs and Ethernet ports: two WAN ports and four switch ports. On the back end you'll find the power input and a serial port for console access. There are no wall mounting holes on the bottom of the unit.

After logging into the web GUI, you see the status page. We didn't find any setup wizards. On the top of the pages, you'll find the main menu and then below that, the sub-menu. And just below that, many of the pages also have several tabs to choose from. Having all three menus shown on top of each other does clutter up the navigation somewhat. However, we did like the provided help and documentation. Each section of settings in the web GUI has a question mark button, which takes you to a pretty thorough description of those settings.

We found this Netgear unit to be an average VPN router without any bells or whistles, although Netgear provides a IPSec VPN client program for simplified client deployment. Keep in mind, the unit lacks client support of PPTP and L2TP, making IPSec the only way to join the unit to perform site-to-site connections.

We also felt this unit could use some improvements to the user-friendliness of the GUI, especially the menu design. Also, when adding VLANs you must manually input all of IP and DHCP settings for the new subnet, similar to the D-Link unit. However most routers automate or preconfigure some of these settings for you.

UTT Technologies HiPER 518

The HiPER 518 has a list price of $69.99, but is currently selling for $59.99. It is one of three different small business routers UTT Technologies offers, one of which is very similar in functionality and the other supporting more WAN connections, VPN tunnels, and additional authentication and billing functionality.

This UTT unit supports up to five concurrent IPSec VPN site-to-site and/or client-to-site tunnels, with a very low advertised throughput rating of 15Mbps. The only other VPN support is the PPTP server and client, supporting up to five concurrent users.

In the box, along with the unit, you'll find an Ethernet cable, power adapter, and a product catalogue. You won't find any install guide or manual, though you can download a manual from their website.

The metal case measures about 7 inches wide, 1 inches high, and 5 inches deep. On the front of the unit are the status lights for the power, system, and WAN/LAN ports. On the back you'll find one port specially for a WAN connection and then four LAN ports, three of which can be used as additional WAN connections. You'll also find the power input and a reset button on the back. On the bottom of the unit are non-stick pads, useful when placing on a desk or shelf, as well as two holes for optional wall mounting.

After logging into the web GUI, you're

FeaturesTable

	Cisco RV325	D-Link DSR-250	DrayTek Vigor2925	Linksys LRT224	Netgear FVS336G	UTT Technologies ER518
Switch Ports	14	8	5	4	4	4
VLAN Tagging	X	X	X	X	X	
WAN Ports	2	1	2	2	2	4
WAN Load Balancing	X	X	X	X	X	X
WAN Failover	X	X	X	X	X	X
USB Ports	2	1	2			
USB WAN Failover	X	X	X			
USB Print Server		X	X			
USB File Server		X	X			
Wired 802.1X	X		X			
PPPoE Server						X
Web Authentication			X			X
VPN Support and Max Simultaneous Tunnels						
IPSec VPN	X	X	X	X	X	X
IPSec Tunnels	50	25	50	45	25	5
SSL VPN Server	X	X	X		X	
SSL VPN Tunnels	10	5	25		10	
OpenVPN Server		X		X		
OpenVPN Client		X		X		
OpenVPN Tunnels		5		5		
PPTP VPN Server	X	X	X	X	X	X
PPTP VPN Client		X	X			X
L2TP Server		X	X		X	
L2TP Client		X	X			
PPTP/L2TP Tunnels	10	25	50	5	25	5
Advertised Max Throughput in Mbps						
IPsec Throughput	100	50	60	110	78	15

prompted with the optional wizard, which only helps to configure the Internet connection. After that, you're taken to the simple system info page showing a couple main stats.

Although the look and design of the web GUI is very basic and simplistic, it is still user-friendly. The main menu is on the left side of the page with expandable categories, displaying shortcuts to all the main pages. Then many of those pages have multiple tabs to view additional settings. Some pages have a Help button that pops up another browser tab to a simple description (many of which could be elaborated more) of the settings of that particular page.

After browsing through the GUI, we found most of the common VPN router features. However, one exception is the lack of VLAN support; you can't define separate VLANs to segregate traffic. Also lacking are the QoS settings. It only allows control over the bandwidth rates, and not priorities. However, the unit does offer a PPPoE server supporting up to 30 users and web authentication for authenticating local users before they're granted Internet access.

We found this UTT unit to be fairly unique. It includes some functionality that the other routers don't, such as a PPPoE server and web authentication. However, at the same time it lacks support for some common features, such as SSL VPN and VLANs. Keep in mind though that other models from UTT do support VLANs along with additional functionality.

Comparing the routers

All the routers have IPSec and PPTP VPN servers and all but two (the Linksys and UTT units) have a SSL VPN server to allow clients access via a web browser. All the routers support both site-to-site and client-to-site tunnels for IPSec, while many of the routers only support client-to-site for some or all of the other VPN protocols.

Each router provides some type of WAN load balancing and failover via either a second WAN port and/or by supporting 3G or 4G wireless USB adapters. All but one (the UTT Technologies unit) provide VLAN tagging support. Two of the routers (the D-Link and DrayTek) also provide simple file and printer sharing via their USB ports. ■

Eric Geier is a freelance tech writer–keep up with his writings on Facebook or Twitter. He's also the founder of NoWiresSecurity providing a cloud-based Wi-Fi security service, and On Spot Techs providing RF site surveying and other IT services.

THE ULTIMATE GUIDE

BY JAMES E. GASKIN

BEST NAS BOXES FOR SMALL BUSINESS

IT'S a good thing storage keeps getting less expensive because we keep needing more of it. And if you're looking for a desktop Network Attached Storage device, the current crop of NAS appliances should make you happy. Every box we tested worked well, provided boatloads of storage, and many cost less today per terabyte than they did just a few years ago.

NetResults

	Qnap TurboNAS TVS-471	Thecus N5810 PR	Zyxel NAS540	ioSafe 214 NAS	Buffalo TS3400D	Netgear ReadyNAS 316	D-Link ShareCenter +4 Cloud Network Storage Enclosure (DNS-340L)
Price	$1,100 (diskless)	$699 (diskless)	$312 (diskless)	$599 (diskless)	4TB $599, 12TB $1,000	$849 (diskless)	$299.99 (diskless)
Pros	• Tons of apps • Can run an entire office	• Tons of apps • More like an SMB server than a storage device	• Easy install • Easy install, good price/ performance	• Ruggedized • Lots of applications	• Easy to set up • Good price • Solid performance	• Tons of storage • Lots of apps	• Small • Stylish • Easy to set up
Cons	• Most expensive in our test	• Not the easiest to set up	• No advanced business apps	• Heavy • Fewer ports and connectors than other products	• No bells and whistles • Not many business apps	• Interface might be a bit dated	• Not a ton of apps

One trend in NAS appliances is to push the boundary and try to become application servers, not just storage devices. Four of these seven units come with enough software, mostly free open source applications, to run a complete small business and provide Web hosting besides. Software options include multiple versions of popular programs like CRMs, Web servers, content management systems for those Web services, and even full accounting and HR packages. Two of them include Asterisk, so your storage box can also host VoIP server software.

The seven products in this review are from QNAP, Thecus, ZyXEL, ioSafe, Buffalo, Netgear and D-Link.

The affordability of surprisingly large drives (2TB drives cost less than 80GB drives did not that long ago) means you can plop dozens of terabytes of storage on the corner of your desk and never notice, or hear it. All the units fit into basic office décor, and none make enough noise to be heard over the fan in your desktop PC and some laptops. All will provide big storage while sporting relatively small price tags.

And the feature list keeps growing. If you're getting into server virtualization, most of these drives can become iSCSI targets and provide shared storage to multiple virtual machines. All will do a great job backing up clients, Macintosh systems as well, and most will happily shuffle the files off to another NAS box in another location for backup and disaster recovery, or be your front end for cloud storage.

Your first, or next, desktop NAS data storage appliance should be one of these boxes profiled here. Many of these vendors have been making storage for decades, plenty long enough for hardware and software to be wrung free of bugs. Others may be new to the NAS market, but have years of network device history behind them.

HERE ARE THE INDIVIDUAL REVIEWS:

QNAP TurboNAS TVS-471

About the size of a small four-slice toaster, the QNAP TurboNAS TVS-471 is one in a big family of NAS appliances from small (single drive) on up to 24-bay rack systems for data centers. If you need one or more disks in a box, QNAP has plenty of choices.

Our four-drive system included 4TB drives for a RAID 5 capacity of 10.89TB (RAID 0, 1, and 6 are supported, as is JBOD). By default, DataVol1 offered half that capacity. There are four 1GB Ethernet ports, five USB ports (three 3.0 and two 2.0), and even a full-sized HDMI port.

Setup used more cloud than usual, including a QR code on the box so you can initiate the setup via smartphone. We didn't, but the QR code opened up the same myQNAPcloud.com site to get rolling as our client PC. We changed the DHCP address to a static IP address, updated the firmware (the QNAP did it all itself), and started with the setup screens.

User setup offers more controls than NAS boxes in the past, as well as integration into a Microsoft Active Directory or Open LDAP structure. You can setup multiple users at a time, a handy touch, and they can all have their own home directory.

Once configured, it was clear the TurboNAS TVS-471 can do far more than just store files. There seem to be more than 100 applications of various kinds, a trend for desktop NAS boxes the last few years. But we've never seen full accounting programs, databases, HR, ERP, and even a Fleet Management app. The web server included 28 different content management programs from Drupal to Joomla to WordPress and many more. Perl, Ruby on Rails, and Python are included in the 16 development tools. The HDMI port comes in handy for some of the 25 entertainment apps, or perhaps the two surveillance programs. And backup from the TurboNAS to Amazon S3 and many other cloud backends are included. Customers getting into virtualization? QNAP supports all the major hypervisors as iSCSI storage. You can even backup LUN block storage devices to this little box.

Seems a shame to call this multi-talented box "merely" a NAS. Web server to dedicated CRM server to Macintosh Time Machine backup system that replicates to other disks for disaster recovery? Needs a bigger name. Add in the remote Web file access and file sync tools, along with more monitoring screens than an early

Windows server, and you have a complete business in a small black and gray box.

Thecus N5810 PRO

This is another box that can power a complete office with tons of capacity (five disk slots) and more available applications free for downloading than any system we've ever seen. The heavy metal box, the dashboard-type finished black plastic on the front, the disk trays out in the open (but locked), all add up to "serious server," and more than just extra network storage.

No "friendly" management icons here – this box is for business, not home users. How business ready? The only NAS appliance we've ever seen with a mini-UPS that loads right into the case. Hard to believe a reseller would install a NAS without a UPS plug available, but just in case....

Five 1GB Ethernet ports, although one also has a WAN label, since the Thecus N5810 PRO supports Virtual Private Networks as both client and server. Five USB ports, with four on the back (two each USB 2.0 and USB 3.0) and another USB 3.0 on the front. There's also an HDMI port (to support the multitude of media servers). Some other boxes have HDMI ports, but no other one in this batch includes a line out for speakers. If you want a media server with giant storage space, this fits the bill.

Only three of the five disk slots were filled in our test unit, but they were filled with 4TB disks (3,726GB usable space each). Configuring them as RAID 5 (usually done with four disks, but three works), we finished with a usable capacity of 7.4TB. Performance was plenty fast with no hiccups or strain evident on the box powered by an Intel Celeron Quad Core processor and 4GB DDR3 RAM.

ISCSI thin provisioning support is included, along with everything necessary to be a storage destination for the three most popular hypervisors: VMware, Citrix, and Microsoft Hyper-V. Cloud backup? Check, to Amazon S3, Elephant-Drive, and Dropbox. If you're going virtual, you're probably using Active Directory, so you'll appreciate the AD and LDAP authentication support. And the snapshot backup support will likely come in handy.

But if you want a general application server that's not from Microsoft, Thecus offers server and application options. When you click the link to download available applications from the Thecus website, you'll find pages and pages and pages of apps of all types. Multiple Web servers, media servers (remember that speaker line

out and HDMI port), CRM, accounting, content management, mail servers, photo servers, and the list keeps going. Businesses today can find every application type in a good Open Source library, and the Thecus N5801 PRO probably has the app you want ready to download and run.

If resellers are looking for a server to handle just about every job a server ever had to deal with, while keeping their inventory low, the Thecus N5801 PRO should be first on their list. Company IT groups looking for some departmental storage will be satisfied. High capacity, high performance, and high flexibility are three good traits in a server.

ZyXEL NAS540

ZyXEL, long a player in network equipment for service providers, businesses, and home, has started a new line of Network Attached Storage appliances. Aimed currently at smaller businesses, the five models support from one drive to four, and focus on personal cloud storage (like the NAS540) or as a Media Server.

Toaster sized, the NAS540 has a plastic shell that supports disk installation without tools and keeps the cost down. Well, you will need a screwdriver to install your choice of 3.5 or 2.5 inch hard drives. All drive capacities are supported, up to the most recent 6TB drives for a grand total of 24TB (without RAID disk redundancy).

Either by being new or by aiming at smaller businesses and home users, the ZyXEL NAS540 includes painless installation and a friendly administration interface. A more traditional but still clean interface hides beneath the "easy" mode. Since the friendly interface doesn't offer many controls, most of the work is done in the traditional look and feel.

Focusing on cost-effective storage and the cloud tools, ZyXEL offers none of the range of business applications included with several of the other products. That said, you can use the NAS540 as a media storage and streaming device and print server. The front USB 3.0 port can support external storage device, or be used to copy files to and from the NAS540 quickly and easily. The SD card port on the unit allows the same quick transfer option. If your still or video camera or audio recording device uses SD cards (most do today), then this quick transfer option may be a big bonus.

Macintosh systems are supported, including with a Time Machine backup server. Default shared folders are admin, music, photo, and video (another clue about the target audience). ITunes, a Web server, WordPress, and a Dropbox sync utility are included. Smartphone access through the cloud using the ZyXEL app make it easy to share files or create a giant security hole depending on your point of view. The most polished app seems to be the Gallery utility for photo display.

The myZyXELcloud remote access and management capabilities make it safe to put this in a customer site without any network computing expertise. While the admin utility is straightforward, small business users may appreciate some help. While it only has 1GB of RAM and a FreeScale Dual Core 1.2 GHz processor, there are few apps to support and the dual 1Gigabit Ethernet ports provide good bandwidth.

ZyXEL has a good reputation in network products so expect to see their new NAS line grow. The NAS540 may lag behind the fancy app features curve, but it offers good storage value in an easy to administer package.

ioSafe 214

The heaviest NAS appliance we have ever seen, the ioSafe 2014 could be used as a boat anchor. And since it's waterproof, your files might actually be safe. Add in the fireproofing, and you have a box for the paranoid boss or customer who doesn't trust the cloud so needs the safest shared storage possible. While we didn't drown or set the ioSafe 214 on fire, the multiple protective internal layers give us confidence the data inside would still be safe no matter what we did to it.

As big as this was, it only held two drives, but the big brother ioSafe 1515+ holds 5 disks. Probably need a wheelbarrow to move that box around. But RAID 1 with mirrored 6TB disks provides some serious storage. Our test unit had dual 1TB drives. There are few connectors – a single 1GB Ethernet port, two USB 3.0 ports in the back and one USB 2.0 port in the front for copying to and from an external drive. This paucity of ports probably has more to do with structural integrity for the box than anything else.

The hardware comes from ioSafe, but the operating system comes from Synology. That makes for some slight confusion early on, but we got used to it quickly. Admin screens are friendly and icon-heavy without being cutesy.

Like many other NAS appliances now, the ioSafe 214 includes multiple applications that turn a shared storage box into a dedicated application server without paying Microsoft software and client licenses. For the ioSafe 214, the packages include Web servers (Tomcat), content management systems (Drupal, Joomla, WordPress), mail servers, media servers, Python, Ruby, OpenERP, OrangeHRM, vtigerCRM, SugarCRM and various media servers. Oh, yes, iTunes and BitTorrent for music, antivirus, and even the Asterisk Internet Phone system software.

Want to block IP addresses with too many failed login attempts? Done. Wireless network support? Just add a USB wireless adapter, and

the OS supports wireless.

The browser-based admin page includes a friendly widget that shows a big green check mark with the word Good along with the server name and network IP address. Below that is a resource monitor showing CPU and RAM use, along with LAN bandwidth used. Small business customers will feel comforted even if experienced admins scoff. But those scoffing admins might smile when they enable the Telnet service for system login.

IoSafe 214 offers an interesting value proposition: built like a tank, literally, to keep your files safe. Despite that, the online backup options and replication tools allow users after the traditional NAS appliance experience to get what they want, too. And no one need fear the worst if they spill coffee near this box.

Buffalo Technologies TS3400D

Say hello to another box in the "lots of affordable space" family. Buffalo Technologies, one of the first in the big-disk desktop NAS market with its initial 1TB appliance, follows the same plan as before: straightforward, simple to setup and administer, and file space forever. At least it seems like that, when a NAS appliance sold through multiple retail outlets offers nearly 5.5TBs of disk space when using four 2GB drives with RAID 5 redundancy.

Setup and configuration screens may look a bit dated, but the user interface has survived the test of time. An odd choice of IP address by default (192.168.11.40) took us by surprise, but it was no harder to change that unusual address to a static IP than any other default address.

The "regular" admin screen has been refreshed over the years, and Buffalo has added an "Easy" page as well. Only thing the Easy page adds is some big, descriptive buttons that when pressed drill down to the specific admin within the regular management program. The friendly icons save a click or two, but that's it. We doubt anyone but the most timid admin will use the Easy interface, but it's there just in case.

Also there are two 1GB Ethernet ports and four USB ports, two 2.0 and two 3.0. External disks can be attached as can printers. The appliance acts as an iSCSI target. A decent but limited list of other goodies include media servers, Web and MySQL servers, replication, a link to Amazon S3, and a WebAccess feature when routed through a BuffaloNAS.com portal.

The box will function as the storage system for surveillance cameras, and include TeraSearch, a rudimentary file indexing search program. Few offer file search anymore, which is probably why Buffalo hasn't felt the competitive need to upgrade their app over the years. It can search only within .txt and .html files. Otherwise it just helps you find filenames based on the text you enter.

NovaBACKUP licenses are included, as is replication to other Buffalo NAS devices, including a Failover option. Apple users can use the Time Machine support for their backups. If you're running an Active Directory domain, the TeraStation TS3400 can fit into that scheme. Otherwise you create users and groups on the box itself, or share a giant pool of storage with everyone on the network in guest mode. That works fine and admins encounter few problems in setup or maintenance.

Flashy? No. Full of disk space for a good price? Absolutely. Hard to go wrong with proven desktop NAS that's been updated but retains the same fundamental stability from back when a single TeraByte in one box made headlines.

Netgear ReadyNAS 316

Another vendor who's been in the desktop NAS business a long time, Netgear's ReadyNAS line covers home and small business, including a rack-mounted model. The ReadyDATA line slants more to business with higher-end features like unlimited snapshots and other data center type goodies. But their most popular model is the ReadyNAS 314 with four drive slots. This box, the 316, holds six disks that can add up to 24TB with the 4TB drives, and more with an optional expansion chassis.

The six-drive models have nice looking and clean fronts with a blank cabinet door holding a backlit display that suddenly shines out of nowhere when you touch the plastic front. Nice design move. Since it holds six drives, this box is bigger than most we tested, but it's quiet and unobtrusive, just like all the other ones. None of them can be heard over even the quietest office background noise, and this model is no exception.

Ports on the box are typical, with one addition. There are two 1GB Ethernet ports, two USB 2.0 ports in back and one in front, and two USB 3.0 ports on the back. There's an HDMI port, and two SATA connectors. Why? Netgear offers an expansion chassis option if you need up to 96TB of desktop NAS.

The Netgear RAIDar utility helps you locate your NAS box on your network. A dated look, perhaps, but the utility still works fine. A set of shared folders, Music, Pictures, and Video are setup by default, with DNLA support. Two Netgear NTP servers are loaded into the NTP server text box so time setting is simple.

A single admin interface does the job. Even though complete, it's clean and simple enough any power user will be able to handle the setup and configuration. Create users, give them access to shared drives, then let them store terabytes of files without problem.

Downloadable apps abound, about 75 or so. All manner of open source apps are included, such as WordPress, Drupal. Joomla, Moodle, various ERPs and CRMs, Asterisk for VoIP phones, surveillance server, and more. A special program is the front end for Egnyte, the cloud-based server as a service company. They made a deal with Netgear to handle the on-premise hardware for customers who want that option.

Netgear storage has always been affordable, and the ReadyNAS 316 continues that trend. Multiple retailers and distributors carry the brand, so they're easy to find. Add all this together, and you get gallons of storage for cupfulls of cash, along with hardware and an operating system that's worked well together for years and years and years.

D-Link ShareCenter +4 Cloud Network Storage Enclosure (DNS-340L)

The smallest, and most stylish, box in this group, the D-Link ShareCenter is another fairly new entry in the market. D-Link, around for years and years, always focused on routers, switches, and the like. Their foray into NAS is welcome, and they've brought some new ideas.

D-Link ShareCenter +4 Cloud Network Storage Enclosure

First is the look. Smallest, and the only one where the disks are inserted from the top down into the unit. No trays, just raw disks, so that cut the size down and made this the smallest box of the group.

Second is the good setup Wizard that will help users unfamiliar with storage devices do multiple setup items they need to do for a working system. When not using the Wizard, the colorful icons make the browser-based admin page look friendly enough that less experienced admins will feel comfortable.

Hardware-wise, this box covered the basics. Dual 1GB Ethernet ports, two USB 2.0 ports on the back and one USB 3.0 port on the front, and 2.743TB of open space from four 1TB disk drives was about right, allowing for RAID 5 redundancy and operating system overhead.

The Setup program on the included optical disk helps the new admin as well. It also includes PC backup software from D-Link that can go to the NAS or the D-Link cloud through the on-site hardware. You can also view the User Manual, all 400-plus pages of it, if you're interested.

This box has an interesting dual personality. On one hand, D-Link is making it consumer friendly with pretty icons and the Setup Wizard. On the other hand, it includes SNMP support for management, iSCSI support, NFS, and even assigns users access to the box via FTP. Interesting mix. And the cloud components include cloud backup, but also syncing with Dropbox and Google Drive. And a front end to the Amazon S3 service, in case you're fronting a huge cloud database with a consumer-friendly NAS appliance.

All was not perfect, but pretty close. D-Link

includes a few applications, but not many. A surveillance server back end if you have one of the many D-Link network cameras, WordPress, Joomla, and a handful of others. But the Add-on Center page, where we were supposed to download the files from the D-Link website, never worked right, complaining about a lack of Internet connection. The D-Link website made it easy to download and install them manually, so we were covered, but it was an odd glitch. We were monitoring the box via the MyDlink.com portal, so the Internet was working.

Minor glitch for a feature few will likely use, and not enough to spoil the experience. Volumes can be encrypted with a click of a checkbox during creation, an odd feature for a small business storage appliance, but perhaps comforting for some users.

Users can be added by linking up to Active Directory, individually, or in a batch. No home directly is created automatically, but it's easy to mark a volume "Read / Write" for everyone for a giant pool of storage to share among a workgroup.

Small businesses without storage experts will have no trouble adding the D-Link ShareCenter to their network. ■

James E. Gaskin writes books, articles, and jokes about technology, and consults for those who don't read his books and articles. james@

THE ULTIMATE GUIDE

BY ERIC GEIER

SOFTWARE-BASED NAS OPTIONS FOR THE STORAGE DO-IT-YOURSELFER

Software-based Network Attached Storage (NAS) is perfect for the do-it-yourselfer who doesn't want to buy a pre-packaged appliance. With software-based NAS, you load the software onto the device of your choice — whether it's a PC, server, or virtual machine. You can even run software-based NAS in the cloud.

For this review, we looked at FreeNAS, NexentaStor, Open-E DSS V7, Openfiler, and SoftNAS Cloud and Windows Storage Server 2012 R2.

FreeNAS, NexentaStor, Open-E and Openfiler can all be installed onto either your own physical machine or virtual machine with their provided ISO disk image. SoftNAS Cloud is limited to deployment on virtual machines or in the cloud.

If you're looking for a free solution that you can use in a production environment, consider FreeNAS, Open-E DSS, or Openfiler, but keep in mind all lack some advanced functionality. FreeNAS and Openfiler don't limit the amount of storage capability, but Open-E does have a 2TB limit for their free edition. If you're looking for a cloud-based solution, SoftNAS Cloud is your best bet. Windows Storage Server is slightly different in that it can only be purchased pre-loaded onto an appliance sold by a number of third-party vendors, but not from Microsoft itself.

HERE ARE THE INDIVIDUAL REVIEWS:

FreeNAS 9.3

FreeNAS is perhaps the most popular free and open source NAS solution, designed for use on home and small business networks. It is developed by iXsystems and derived from the Unix-like OS, FreeBSD. In addition to the downloadable ISO disk image that can be used to install on your own hardware or virtual machine, they offer preinstalled appliances. They also develop and sell a similar solution called TrueNAS, which includes additional

NetResults

	FreeNAS 9.3	NexentaStor 4	Open-E DSS V7	Openfiler 2.9	SoftNAS Cloud 3.3	Windows Storage Server 2012 R2
Free Licensing / Storage	BSD License / Unlimited	Non-commercial / 18TB	Proprietary / 2TB	GNU GPL v2 / Unlimited	Proprietary / 1TB	n/a
Commercial Starting Price / Storage	n/a	$1,725 / 8TB	$895 / 4TB	$1,010 / Unlimited	$119 per month / 1TB	n/a
Pros	• Wide variety of deployment options. • Supports encryption	• User friendly web GUI • Thorough documentation	• Wide variety of file sharing protocols • Convenient help shortcuts	• Unlimited storage limits • Supports multiple file systems	• Full cloud-based support • Quick deployment	• Supports encryption • Familiar Windows Server GUI
Cons	• Lacks failover and Fibre Channel support	• Free edition lacks HA and replication • No hardware RAID support	• Lacks deduplication and compression	• Free edition lacks HA and Fibre Channel • Documentation lacking.	• No quick help shortcuts	• Unavailable for install on your own machine

functionality and commercial support designed for critical business and enterprise applications.

Beginning with version 9.3, FreeNAS only supports 64-bit processors. The minimum recommended amount of RAM is 8GB. A flash, SSD, or hard drive of at least 16GB is required for installing the OS onto, in addition to at least two other (non-RAID) drives for storage.

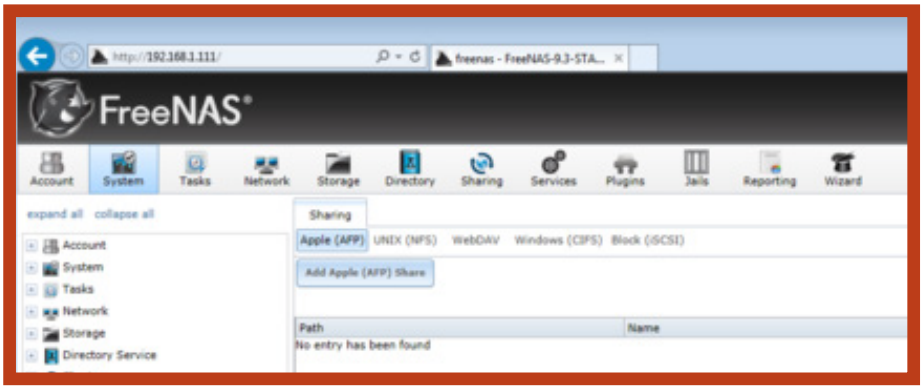
FreeNAS uses ZFS and offers the typical benefits of that file system, including snapshots and software-based RAID. It's one of the only NAS solutions also offering AES-XTS encryption. It provides the usual file sharing protocols, supports the typical user authentication directories, and includes all basic NAS functionality. Plus you can add features such as cloud backup of the storage via plug-ins developed by third parties.

FreeNAS also acts as the server for the following PC backup clients: Windows Backup, Apple Time Machine, Rsync, PC-BSD Life Preserver, and via a plug-in, Bacula. For backing up the NAS storage, there are plug-ins enabling backups to both CrashPlan and Amazon S3. There are also plug-ins available to provide additional functionality, such as torrent and other Internet file sharing and media server and streaming features.

It's worth noting that FreeNAS does lack two advanced features seen in most other solutions: high availability or failover functionality and native Fibre Channel support. Both of these features are available in the commercial TrueNAS offerings.

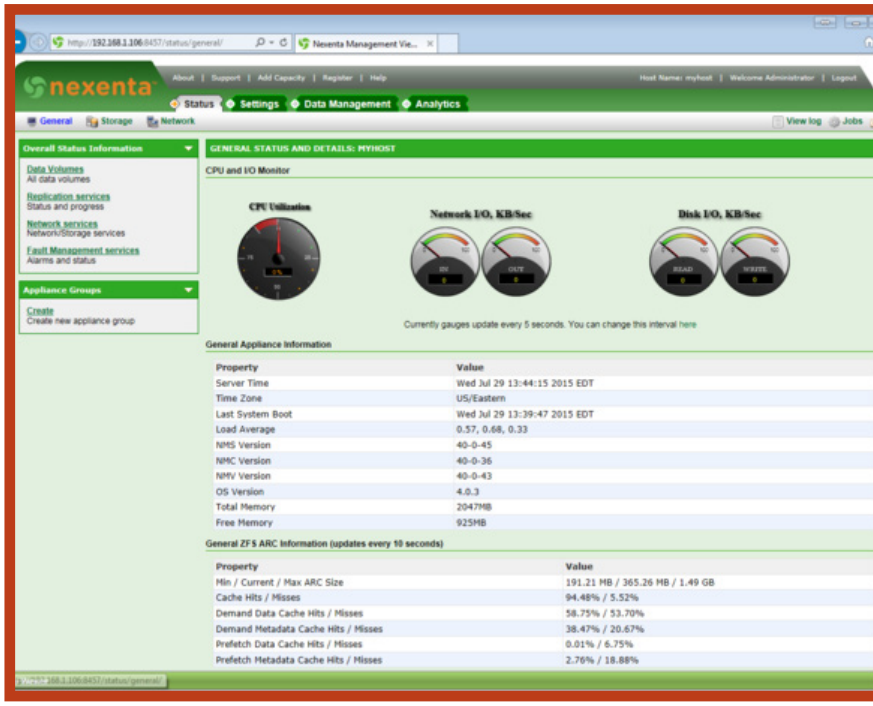
After booting up a machine with the provided disk image, you're presented with a simple DOS-like installation. You choose the install location and set a root password. Once FreeNAS starts, you see the Console Setup screen. In addition to displaying the IP where you can access the web GUI, you can utilize the console to configure the network settings, reset the password, restore factory defaults, apply updates, backup/restore the configuration, and reboot or shutdown the machine. You can also access the raw shell.

After logging into the web GUI, a wizard prompts you to configure the basic settings, including regional settings, disk and RAID configuration, and a directory service for authentication. After clicking around the web GUI, we found it user-friendly and attractive. You can navigate to the main screens by clicking the icons on top of the page and then choose a tab for specific settings. You can alternatively utilize the expandable list on the left to directly access all screens, pages and functions.



From any page, you'll find a Support, Guide, and Alert button in the upper right of the screen. The Support button takes you to a web form where you can create a bug report or

feature request. The Guide button takes you to the beginning of their web-based user guide, which is well-written. The Alert button serves as a LED status light, which will change color when alerts are active, and clicking the button.



NexentaStor 4

NexentaStor is available as a free community edition with limitations for non-commercial use and as a commercial enterprise edition. We evaluated the enterprise edition with their publicly available 45-day trial. Pricing starts at $1,725 for up to 8TB. Both editions are based on the IllumOS and can be installed on bare metal via their IOS disk image or on virtual machines via their VMware or XenServer images. The developer, Nexenta Systems, also offers other cloud-based and virtual storage solutions.

They recommend installing on a physical or virtual machine with a 64-bit processor with a minimum of 8GB of RAM plus 1GB RAM per 1TB of storage space. Two identical small disks are required for the optional high-availability system folder. Storage disks cannot be implemented via hardware RAID.

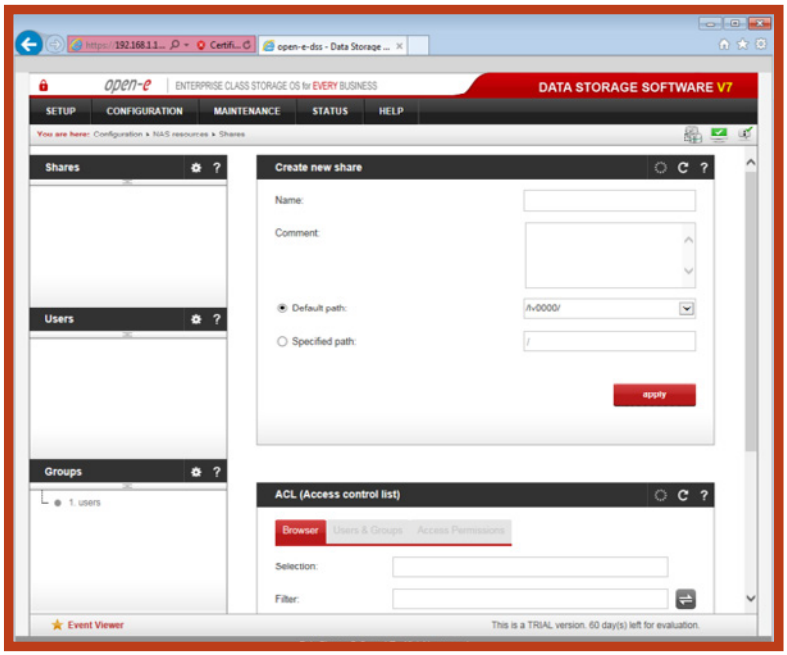
NexentaStor is a ZFS-based solution, offering the typical ZFS features, such as snapshots and software-based RAID. It provides the most popular file sharing protocols, but does lack some, such as AFP and WebDAV. It supports the typical user authentication directories and includes all basic NAS functionality. The free Community edition, however, is limited up to 18TB of storage and doesn't include high availability or replication functionality.

After booting from the IOS disk image, the DOS-like installer will prompt you to accept the license, set region/location settings, and choose an install location. At startup, you must accept the terms and complete the registration. Next, you're prompted to configure the web GUI protocol (HTTP or HTTPS) and port. Finally, you're presented with the web GUI address.

The first time you visit the web GUI, you're prompted with the setup wizard to configure the network configuration, admin passwords, and email settings for the notification system, iSCSI parameters, disk and volume configurations, and folders and shares. Once you're done you can review the changes and start the server.

The web GUI is a multi-tabbed interface with

the main tabs on the top menu and sub-tabs below that. There's a menu for the sub-tabs on the left portion of the screen as well. On the very top of the web GUI, you'll find some links, including a Help link that takes you to the beginning of their thorough web-based documentation.



Open-E DSS V7

Open-E DSS (Data Software Storage) V7 is one of the two software-based storage solutions Open-E offers, designed for SMB and Enterprise environments. It is the more entry-level offering of the two, with a recommended total storage capacity of 200TB. They offer a fully functional 60-day free trial and pricing starts at $895 for up to 4TB storage. They also offer a free Lite version that lacks some functionality, including Fibre Channel, hardware RAID, and volume replication, and has a 2TB storage limit.

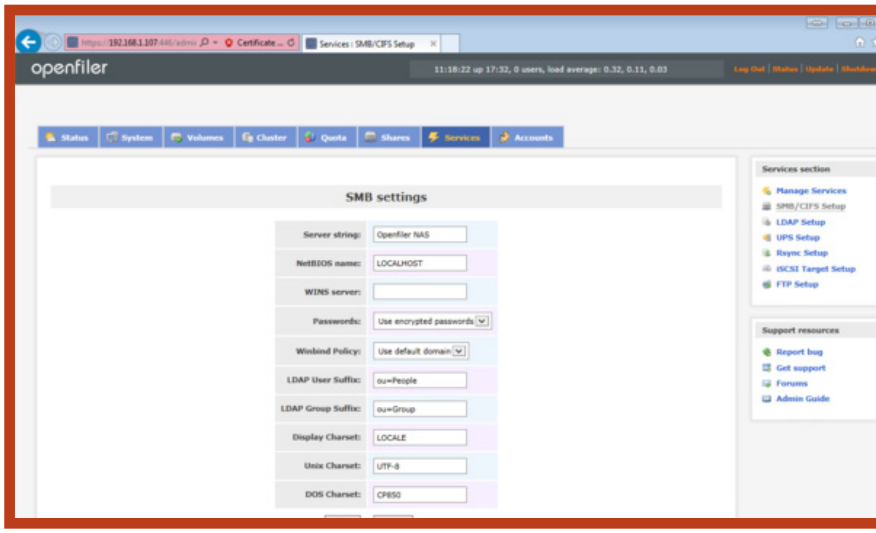
Open-E DSS requires a 64-bit processor and at least a 2GB drive for the OS and 4GB of RAM. They provide an ISO image for virtual deployments or to burn a disc for physical machines. They also provide downloadable zip package in order to create a bootable USB flash drive. Both options can be used to install either of the three different versions of the solution.

Open-E DSS is an XFS-based unified storage operating system, offering all the basic NAS capabilities, including the typical file sharing protocols and user authentication support. The only common sharing protocol lacking is WebDAV. Its iSCSI active-active load balanced failover adds extra performance for demanding installations. It supports RAID0, RAID1, RAID5, and RAID6 configurations. Snapshots are supported, but limited to 20. Additionally, it lacks some storage drive functionality, such as deduplication and compression, found in their other solution and others with ZFS.

We installed the Open-E DSS Trial onto a virtual machine using the IOS image. We found a DOS-like interface where you simply accept the terms and choose an install location. Then you can connect to web-based GUI, enter a product key for the 60-day trial, free Lite version, or purchase the full version. Then a wizard prompts you to configure the language, password, optionally modify IP/DNS settings, set the time zone and time/date, and define a server name.

Once you access the main web GUI, you'll find the menu on top, giving you a drop-down menu of pages and functions when hovering over the

main categories. In the upper-right of each section of settings is a question mark that you can conveniently click to popup a window with the documentation regarding those settings. From that popup, or by clicking Help from the main menu, you can also search or browse the documentation.



Openfiler 2.9

Openfiler provides a free open source NAS solution and commercial editions starting at $1,010 with more functionality. It was originally started by Xinit Systems and now maintained by Openfiler Ltd (UK). The open source edition is released under the GNU General Public License version 2. The current release is based on the Linux 2.6 kernel and the rPath Linux distribution, compatible with industry standard server hardware or virtual platform. However, the platform has reached its end-of-life and they're working on transitioning to a new base OS: CentOS 7.

Openfiler requires a 64-bit processor, 4GB of RAM, and 12GB for the OS installation. Hardware RAID controllers are supported in addition to the following software RAID modes: RAID0, RAID1, RAID5, RAID6, RAID10. They provide an ISO image for installation on your server or virtual machine.

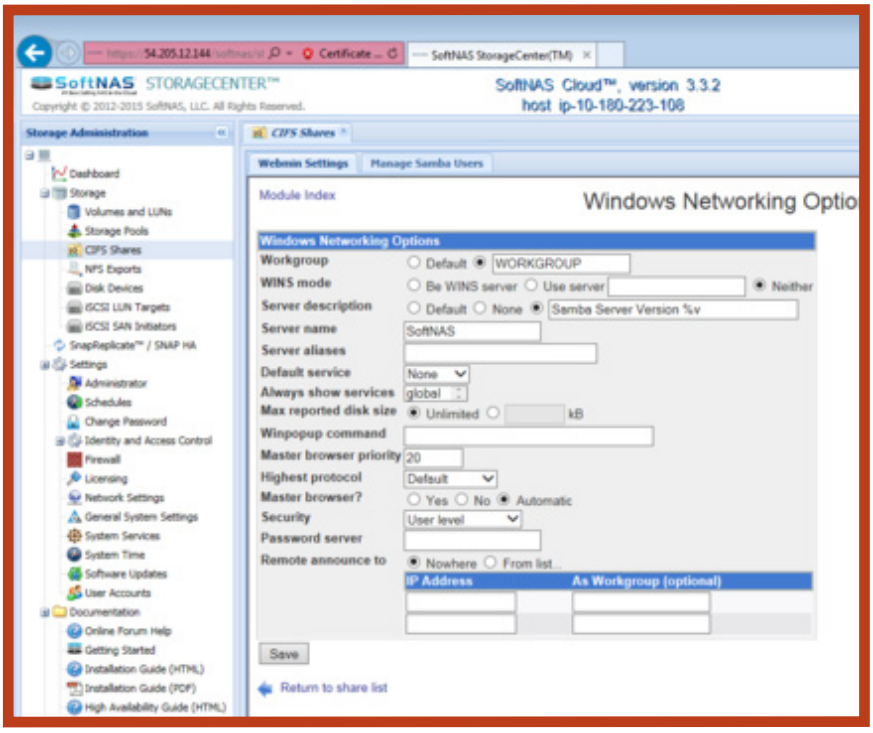
Openfiler supports multiple file systems, including XFS and ext3. All editions support basic iSCSI, snapshots, usual authentication protocols, and other basic NAS/SAN functionality. The popular file protocols and services are supported, except for AFP. Advanced features such as Fibre Channel target, iSCSI Target for Virtualization (iSCSI SAN-4-V), high availability (HA) and block replication, and WAN replication capability for remote disaster recovery (DR), require an SME or Enterprise Subscription and the relevant software feature extensions.

To install Openfiler you can choose between a GUI or text-based install of Openfiler. We did the GUI option, which prompted us for the keyboard type, partition and drive options, IP/DNS settings, time zone, and root password. Then it booted to DOS-like screen showing the IP for web GUI.

The first time logging into the web GUI you're prompted with a wizard to set the volume quota, password, and language settings. Once you reach the main GUI, you'll find a tabbed screen with the main menu on the top and then on most screens you'll find a sub-menu on the right of the screen.

Just below the sub-menu on the left of each screen is also a menu of links to Support Resources, but none led directly to the help or documentation on the particular settings of that

screen. Plus the Admin Guide link was dead.



SoftNAS Cloud 3.3

SoftNAS differs from the other solutions reviewed here by offering the ability to deploy their software both on-premise with virtual machine images using Microsoft Hyper-V or VMware vSphere and in the cloud using Amazon EC2, Microsoft Azure, or VMware vCloud Air. We evaluated SoftNAS via an Amazon EC2 instance.

SoftNAS is offered in three editions. SoftNAS Cloud Express has a 1TB limit, which is free to use on micro Amazon EC2 instances, although any AWS infrastructure charges still apply. Pricing for larger instances and the other editions vary depending upon the platform you use. SoftNAS Standard has a storage limit of 10T to 20TB depending upon the platform, while the Enterprise edition supports more.

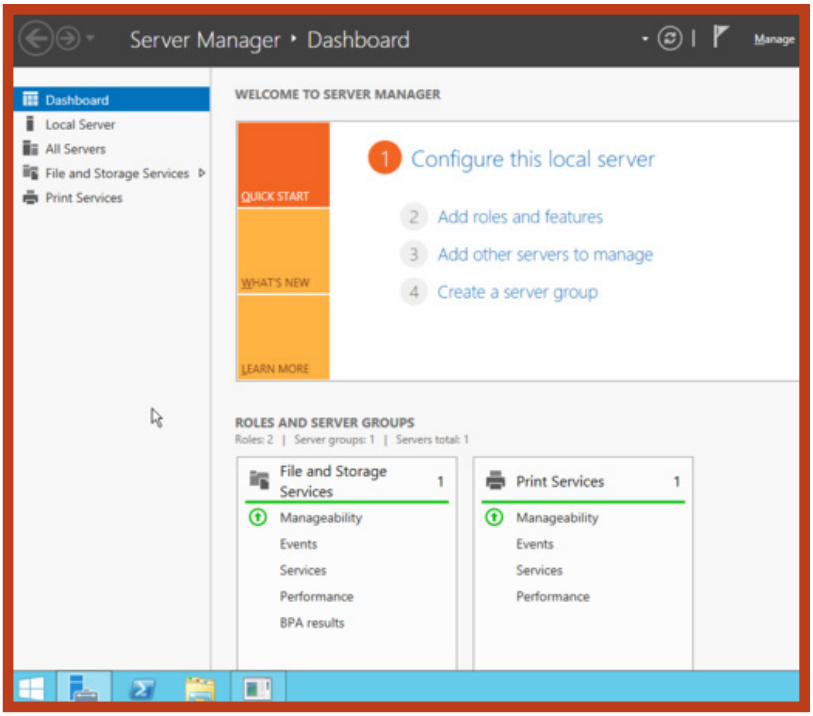
Commonly, SoftNAS Cloud is deployed in AWS VPCs serving files to EC2 based servers within the same VPCs. SoftNAS also supports a hybrid cloud model where one SoftNAS instance is deployed on-premise on a local PC in your office and a second instance in an AWS VPC. In this hybrid model, replication occurs from the local SoftNAS to cloud-based SoftNAS for cloud-based disaster recovery.

SoftNAS Cloud is based on CentOS Linux and utilizes ZFS, thus it offers the usual functionality of that file system, such as snapshots and software-based RAID. It supports the basic file sharing protocols, such as SMB, NFS, iSCSI, and Fibre Channel. Though FTP and WebDAV aren't supported out-of-the-box, they can be easily added by a Linux administrator.

Once we configured the EC2 instance of SoftNAS, we could access the web GUI, which they call the SoftNAS StorageCenter, via the Amazon IP or DNS address. After logging in, you're prompted to register and accept the terms. Then you're presented with a Getting Started Checklist, which is useful in ensuring you get everything setup.

The SoftNAS StorageCenter has a tabbed GUI. The full menu is on the left pane. Clicking a shortcut from the collapsible list opens up the

page in a new tab, allowing quick access to any other tabs already opened. Getting around the GUI is straightforward and user-friendly. There are no shortcuts for quick help on configuring settings, but the main menu on the left pane has shortcuts to all the documentation.



Windows Storage Server2012 R2

Microsoft's Windows Storage Server 2012 R2 is based off of Windows Server 2012 R2, but is specifically designed to serve as a NAS solution. It is offered in three editions: Essentials, Workgroup, and Standard. All offer basic NAS functionality and Microsoft-specific features, such as Storage Spaces (a RAID alternative) and Work Folders. Since it's a Windows OS, you can install any other Windows-based applications and servers as well.

The Windows Storage Server software isn't sold individually, but offered pre-installed on hardware from a variety of vendors such as Thecus, Dell, Seagate, Western Digital, and Buffalo. Pricing for a 2-bay NAS appliance running Windows Storage Server starts around the $300 to $400 range.

Essentials is the entry-level edition, designed for SOHO and small business environments. It includes the Windows Server Essentials Experience, which provides additional functionality such as a simplified dashboard for management and cloud-based access and backup, great for those without Windows Server experience. Given that Essentials is for smaller deployments, it lacks some advanced features such as failover clustering and Hyper-V support. While at the same time, it includes some functionality not seen in the other editions, such as being able to run as an Active Directory Domain Controller, which many smaller networks might not yet have.

The Workgroup edition offers a similar feature-set that of the Essentials edition, but supports more users. Both the Workgroup and Standard editions lack the Windows Server Essentials Experience and Domain Controller ability. The Standard edition adds more advanced support, including data deduplication, Hyper-V, and failover clustering.

All of the common file sharing protocols are supported natively in all Windows Storage

Server 2012 R2 editions, except the Apple AFP protocol, which could even be added via a third-party Windows-based application.

We installed the Standard edition of Windows Storage Server 2012 R2 onto a virtual machine via an ISO image file provided via MSDN. The install process resembled that of a typical Windows OS install. After booting to the ISO image, we had to configure the regional settings, enter a product key, accept the license terms, select an install type, and choose an install disk. Once installed, we were prompted to create an admin password.

After booting into the OS, you'll find the same look and feel of a full Windows Server along with a Server Manager to add, remove, and manage roles. You can use the physical machine where the OS is installed to perform the configuration and management, or utilize Remote Desktop to access the OS elsewhere or remotely manage via a CLI with PowerShell. ■

Eric Geier is a freelance tech writer–keep up with his writings on Facebook or Twitter. He's also the founder of NoWiresSecurity providing a cloud-based Wi-Fi security service, and On Spot Techs providing RF site surveying and other IT services.

FeaturesTables

	FreeNAS 9.3	NexentaStor 4	Open-E DSS V7	Openfiler 2.9	SoftNAS Cloud 3.3	Windows Storage Server 2012 R2
RECOMMENDED MINIMUM SYSTEM SPECS						
Processor	64-bit	64-bit	64-bit	$64-bit	$1164-bit	64-bit
OS Drive	8GB	8GB	2GB	12GB	30GB	32GB
RAM	8GB	8GB	4GB	4GB	4GB	2GB
PROVIDED DEPLOYMENT OPTIONS						
ISO Image	X	X	X	X		
USB Drive Image	X		X			
VM Image	X	X			X	
Cloud Images					X	

Recommended minimum system specs and feature comparison (an "X" means it's included/supported)

THE ULTIMATE GUIDE

BY ERIC GEIER

4 NEW ACCESS POINTS DELIVER SUPER-FAST WIFI

Continuing our ongoing series of 802.11ac reviews, we put four new access points to the test, bringing our total to 13.

This time around, we looked at products from Linksys, Xclaim, Amped and ZyXel, using the same test-bed and methods as our last review.

The Linksys LAPAC1750PRO, which is targeted at SMBs, performed the best in the throughput tests and was a feature-rich product. The Amped Wireless access point was a close second in the speed tests and is a solid business-class access point.

Next was the Xclaim unit, which did well given it's a two stream (2x2) access point, whereas the others are three stream (3x3). This new brand, which was started by Ruckus Wireless, and is targeted towards small office or home office (SOHO) environments, tries to simplify small wireless network administration, but it doesn't offer documentation or flexible admin access.

Coming in last in our throughput tests was the ZyXEL unit. However, it is targeted

towards enterprises and has a number of advanced features in the areas of configuration, management and security.

HERE ARE THE INDIVIDUAL REVIEWS:

Amped Wireless APR175P

Targeted at the SMB market, the Amped Wireless APR175P bills itself as a high-power long range access point. Priced at $299.99, it is a dual-band three stream (3x3) 802.11ac access point, offering theoretical data rates up to 1,300Mbps for 802.11ac. In our testing, the maximum throughput was 335.6Mbps.

This is the only access point in the review that sports external antennas, which provides for either ceiling or wall mounting. In addition to the three 3dBi gain external antenna, it packs a total of six high power amplifiers and six wireless reception (low noise) amplifiers. Its white plastic casing measures approximately 7 square and 1 ¼ inches high, excluding the external antennas.

This Amped Wireless access point has more of a router look and feel. On the top/front, the unit has LED status lights—eight in all—for pretty much every component. Then on one of the sides are all the ports and buttons: power switch, WPS button, reset button, USB port, USB eject button, two Gigabit Ethernet ports, an Ethernet console port, and the AC power jack. One of the Gigabit Ethernet ports is a non-PoE port for LAN connection and the other is PoE capable and can be used for a WAN or LAN connection.

The unit came with an AC adapter, mounting kit, and a relatively big Setup Guide. When you power on the access point, it tries to get an IP via DHCP before setting itself with a default static IP. When you bring up the web-based configuration GUI, you won't find a setup wizard, but the process is straightforward

NetResults

	Amped Wireless APR175P	Linksy LAPAC1750PRO	Xclaim Xi-3	ZyXEL WAC6503D-S
Price	$299	$499	$199	$899
Pros	Built-in RADIUS server; Good in throughput tets	Built-in controller supports 16 APs; Captive portals	Simplifies configuration; Low priced	Automatic provisioning with controller; Wireless Optimizer (ZWO)
Cons	Lacks captive portal and band steering	Built-in controller doesn't support overriding settings	Only configuration via mobile app; No documentation	Poor in throughput tests

and you can click a button on each page for an explanation of the settings.

This access point is the only one in the review that supports a router mode among the typical access point and WDS wireless modes. Additionally, it's the only one that specifically touts being long range and high-power at 500mW output.

The built-in controller functionality supports the central management of up to seven access points. Once you enable an access point to be the AP Controller or Managed access point, the GUI menu is changed, adding new settings for configuring the managed access points. Those you set up as Managed access points will automatically sync with the AP Controller once you make the setting change in the GUI. On both the AP Controller and Managed access points, you can override specific settings of individual access points if needed.

This access point allows you to create up to 32 SSIDs with VLAN support. Among the usual access point features, this unit offers simple load balancing and an intrusion detection system (when in router mode). It also offers an internal RADIUS server supporting the PEAP and TLS methods of 802.1X authentication, enabling the use of the Enterprise mode of WPA2 security.

The access point also provides some convenient features not seen in many access points. A graphical mapping and analytics feature is available when running in the AP Controller mode. You can add floor plan maps, place access points on the map, and visualize coverage better. The access point also allows you to locate the units throughout the building by initializing an audible alarm and LED flashing via the GUI.

Overall, we found this Amped Wireless AP offers some great features, but would be even better if it had captive portal and band steering functionally. In the throughput testing, the access point came in second out of the four access points in this review and sixth out of the 13 APs that we've reviewed.

Linksys LAPAC1750PRO

The Linksys LAPAC1750PRO is targeted towards small and midsized businesses (SMB) and is priced at $499.99. It is a dual-band three stream (3x3) 802.11ac access point, offering theoretical data rates up to 1,300Mbps for 802.11ac. In our testing, it maxxed out at 436.3Mbps.

The front of the Linksys unit only bears a single large LED light, which can change colors to indicate different statuses. This Linksys unit is a ceiling or wall mount type with a look similar to a smoke detector, but its white plastic body is hexagon shaped with curved corners. It's roughly 9 ½ inches round and less than 2 inches high and weighs just over a pound. Inside the unit are three 4.4 dBi internal antennas for 2.4GHz and three 5.2 dBi gain antennas for 5GHz. On the back of the unit are two PoE Gigabit Ethernet ports (one with PoE),

AC power jack, and a small reset button.

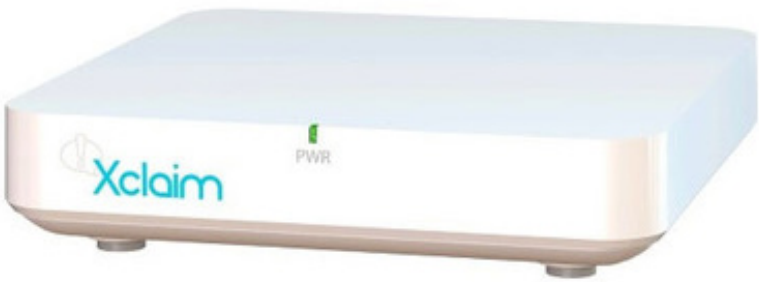
In the box, you'll find an AC power adapter, Ethernet cable, Quick Start Guide, CD with full documentation, and mounting kit. During configuration, we found this Linksys unit first tries to get an IP via DHCP, and if not found it uses a default static IP. Once we logged into the web-based interface, we found a typical tabbed GUI. Though we weren't met with a setup wizard, configuration was straightforward and clicking the Help link would bring up a full explanation of each setting.

When using the Cluster feature, you can centrally manage up to 16 access points using the built-in controller functionality. Once you enable the clustering feature on one access point, other access points will join that cluster. You can centrally change the configuration settings of the cluster via any access point in the cluster. To view status and logs of a particular access point or to configure some individual settings that aren't synced, you must bring up that particular access point's web-based GUI. There's not an ability to override the settings that are synced among the cluster on individual access points.

During our evaluation, we found this unit supports the use of up to 16 SSIDs with VLAN support. In addition to traditional AP mode, you can use the unit in WDS and workgroup bridge modes. Its Captive Portal feature supports guest, local, and external RADIUS authentication and can do URL redirection upon authentication.

We were pleased that this access point supports rogue access point detection, band steering, and beamforming. It also has basic load balancing functionality provided by their Bandwidth Utilization feature. The Packet Capture feature allows you to remotely collect the wireless packets seen by the access point with the ability to filter out beacons, filter using a MAC address, and ability to capture in promiscuous mode.

There's not much to complain about on this Linksys access point. It's feature-rich and did well in the throughput tests coming in first out of these four access points and fifth overall.



Xclaim Xi-3

The Xclaim Xi-3 from Ruckus Wireless retails for $199 and is targeted towards small businesses and small office/home office (SOHO) environments and to the non-IT users. It's the only two stream (2x2) access point in this review, thus naturally offering lower maximum data rates than the other access points: up to 867Mbps for 802.11ac. It hit 315.7Mbps in our testing.

The Xclaim unit has a look and feel between a consumer router and a business access point. It has a white body measuring just over 6 inches square with a height of about 1 ½ inches. Weighing under a pound, this unit is the lightest of the access points in this round-up. Inside are two dual-band antennas, 3 dBi gain for 2.4 GHz and 4 dBi for 5 GHz.

On the back/bottom of the access point you'll

find one PoE LAN port, a secondary Ethernet port, small reset button, and an AC power jack. On the back/bottom of the Xclaim access point are the typical access point ports and buttons. Along with the unit in the box, you'll find a PoE injector, mounting kit, and a simple getting started guide.

Unlike most other business-class products, this unit is primarily designed to be setup and managed via a mobile app, called Harmony for Xclaim. It's available for both iOS and Android devices, and allows you to configure the access point settings when connected to the same Wi-Fi network. There is traditional web-based admin access provided, which you can login locally or remotely. Additionally, according to Xclaim, cloud-based configuration is coming in the future with a software update.

Upon the first opening of the Harmony app, it prompts you to create an admin password, SSID, and a passphrase for the wireless security. Once in the app, you can further modify the wireless settings and create any additional SSIDs.

To setup access points, it searches for and lists all the Xclaim access points on the network you're currently connected to. You can click on each access point to set them up, giving them a name, location, IP details, channel info, and assign them to the desired WLAN(s).

This Xclaim unit only provides the traditional AP mode; no WDS or wireless bridging supported. The built-in controller functionality offers central management via the mobile app with a recommended maximum of 10 access points. You can create up to four SSIDs per access point with VLAN support. As far as advanced features, the unit has band steering, an enhanced QoS functionality called automatic traffic prioritization, and a feature called airtime fairness to help curve the negative impact from older or slower devices.

Beyond the very basic network and access point settings, you'll only find a couple settings to configure: SSID broadcasting, VLAN ID, client isolation, and bandwidth limits (up and down link). Currently you won't find other advanced settings or the ability to use the enterprise mode of Wi-Fi security.

The streamlined configuration interface of the Xclaim products might first appear more user-friendly by non-IT people than the typical web-based GUI of other business-class access points and routers. However, without any documentation on how to use the app or any explanation of the settings, I could see non-IT people actually being confused. They may not understand the few settings that are configurable with the app. Xclaim has an online public forum where you may find answers to your questions, but we don't see this as an acceptable replacement for official documentation or support.

ZyXEL WAC6503D-S

The ZyXel WAC6503D-S, priced at $899, is targeted towards the enterprise-level market. It is a three stream (3x3) 802.11ac access point and is from their Smart Antenna series. Like the other three stream access points, this unit offers theoretical data rates up to 1,300Mbps for 802.11ac and 450Mbps for 802.11n. However,

in our testing, it only reached 232.6Mbps.

Each of the three units in the WAC6500 series are designed for ceiling mounting, with the smoke detector look and feel. The circular housing measures about 9 inches in diameter and about 2.5 inches high. This unit weighs in at just over two pounds. The particular unit we tested has three internal antennas per band, with 4dBi gain for 24GHz and 6dBi for 5GHz.

On the front/top of the access point you'll find seven LED status lights. On the back/bottom you'll find three Ethernet ports: PoE port for uplink, secondary LAN port, and one for console access. You'll find a small reset button and AC power jack as well.

In the box you'll find a Quick Start Guide and mounting kit in addition to the access point. No AC adapter or PoE injector is included; they must be purchased separately if needed.

When you plug the access point into the network, it tries to get an IP address before auto assigning itself a default address. If their separate WLAN controller is on the network in the same subnet, the access point will automatically provision itself. When configuring in standalone AP mode, you'll find a typical enterprise looking GUI with profile-based configuration. It has an online help link on the header of each page, but it doesn't open directly to the details on current page.

This is the only access point in this round-up review that doesn't have built-in controller functionality. A separate NXC Series WLAN controller is required for full central management capabilities. However, there are two PC applications provided by ZyXEL free of charge that allow some management and batch configuration capabilities without a separate controller: the ZyXEL One Network Utility (ZON Utility) and ZyXEL AP Configurator.

In addition to the regular AP mode, this access point currently supports WDS and a monitor mode for rogue access point detection. In the future with a firmware upgrade, the access point will support an interesting wireless mesh technology they call ZyMesh when used with their WLAN controller.

This ZyXEL AP supports up to 16 SSIDs with VLAN support. It has load balancing and band steering functionality. It also has a built-in rouge access point detection feature, but requires exclusive use of either radio. There's no built-in captive portal on the access point, but it is supported when using their separate WLAN controller.

This AP series has what the company calls its Smart Antenna technology, which dynamically chooses the best of more than 700 antenna patterns to use for transmitting to individual clients. The goal is to optimize the physical-layer paths in order to increase performance and reduce interference. Basically they say it's a better alternative to beamforming as their technology doesn't rely on client support.

The ZyXEL Wireless Optimizer (ZWO) software is also provided free of charge by the vendor, which is a mapped-based Wi-Fi simulation, planning, and surveying tool compatible with their access points. It's their proprietary software, basically a very simplified version of other surveying tools like AirMagnet Survey and Ekahau Site Survey.

Although this ZyXEL access point didn't perform well in our throughput tests, it's comparable to other enterprise-class access points in regards to the price and feature-

set. Though it doesn't have built-in controller functionality, it can be used in standalone mode without requiring a separate controller.

How we tested 802.11ac Access Point performance

As in our most previous review, we used IxChariot to run throughput tests on the access points with the same three clients:

- **ASUS PCE-AC66 Dual-band Wireless PCI-E Adapter** (three stream 802.11ac) connected inside the Windows 7 PC, using the provided antennas attached directly to the adapter on the back of the PC tower rather than using their base extender.
- **Netgear A6200** (two stream 802.11ac) plugged into a USB 2.0 port on the back of the same Windows 7 PC.
- **Samsung Galaxy S5** (two stream 802.11ac) Android phone sat on top of the same PC during testing.

On the access points, we enabled WPA2/AES security and 80 MHz channel-width support, and set the 5Ghz channel to 153. All wired connections between the access points, wireless controllers, and testing endpoints were made via Gigabit Ethernet with Cat-6 cables. These connections were all tested and confirmed to be running near Gigabit speeds. During the testing, the distance between the access points and clients was about 25 feet with one wall and a closet partially blocking the line of sight (both made of drywall material).

We ran the tests with the IxChariot High_Performance_Throughput.scr script for one minute with each client individually in the 5GHz band. We simultaneously tested both the TCP uplink (client to access point) and downlink (access point to client), which we add to show the total simultaneous throughput. We ran each access point/client test three times and recorded the average and maximum throughput for each. ■

Eric Geier is a freelance tech writer–keep up with his writings on Facebook or Twitter. He's also the founder of NoWiresSecurity providing a cloud-based Wi-Fi security service, and On Spot Techs providing RF site surveying and other IT services.

PerformanceChart

This chart shows average and maximum throughput in Mbps for each access point connecting via each of our three client devices.

	Linksys LAPAC1750PRO		Xclaim Xi-3		Amped Wireless APR175P		ZyXEL WAC6503D-S	
	AVERAGE	MAX	AVERAGE	MAX	AVERAGE	MAX	AVERAGE	MAX
ASUS PCE-AC66	292.3	436.3	195.7	315.7	247.0	335.6	160.6	232.6
Netgear A6200	167.6	243.1	183.2	262.0	194.9	276.3	151.7	210.9
Galaxy S5	179.6	296.0	163.5	264.8	197.5	331.4	176.4	280.4

THE ULTIMATE GUIDE

BY ERIC GEIER

GIGABIT WI-FI ACCESS POINTS FOR SMBS

Last year we reviewed five of the first Gigabit Wi-Fi access points to hit the market. This time around, we're testing three new entrants: the Cisco WAP371, D-Link's DAP-2695, and the Edimax WAP-1750.

Each product is a three-stream (3x3) 802.11ac access point designed for small and mid-sized business (SMB) environments and

NET RESULTS

	Cisco WAP371	D-Link DAP-2695	Edimax WAP-1750
Price	$399	$389	$279
Pros	Highly configurable, captive portal, band steering, setup wizard	Built-in controller, supports up to 32 APs, band steering	Fastest, RADIUS server, PoE output for additional devices
Cons	Performed slowest No RADIUS server	Lacks setup wizard	Lacks band steering and captive portal, no on-screen help

up. Each includes a built-in controller to centrally manage multiple access points.

The Cisco unit cost the most and was the slowest in our throughput tests, but it was also the easiest to set up and came packed with useful features. The WAP371 offers a setup wizard, built-in controller for up to eight access points, great captive portal functionality, band steering, and packet capture. (Captive portal functionality is used to set up guest users, band steering helps with performance and packet capture is useful for troubleshooting.)

Priced $10 less than the Cisco access point, the D-Link access point offered good throughput results, a built-in controller supporting up to 32 access points, band steering, and advanced security functionality. However, the product lacked a setup wizard. (Watch the slideshow version of this review.)

We found the Edimax unit to be the least expensive and fastest and had a built-in controller supporting up to eight access points, plus it had an internal RADIUS server. While including some relatively unique features, such as Power Over Ethernet (PoE) and a built-in beeper to help locate the access point, it lacked two fairly common features: band steering and captive portal. However, Edimax says both are coming in the next update.

HERE ARE THE INDIVIDUAL REVIEWS:

Cisco WAP371

The Cisco WAP371 is targeted for small-to-midsize business (SMB) environments and is priced at $399. It contains one three-stream (3x3) 5GHz radio, supporting theoretical data rates up to 1,300Mbps for 802.11ac and 450Mbps for 802.11n, and one two-stream (2x2) radio for 2.4GHz. The recommended number of active users is 64 per access point or up to 40 users per band/radio.

On one side, there's a PoE Gigabit LAN port, a reset button, optional AC power input, and a power button.

This Cisco unit has a white plastic body, which is square shaped with curved corners, measuring about 9 inches long and wide and about 1.7 inches tall. At just under 2 lbs, it's lighter than the metal D-Link unit, but heavier than the Edimax unit. Unlike the other two APs, there are no visible antennas, but there's two 2dBi antennas inside the unit. On the top/front there are three basic LED status lights.

On one side, there's a PoE Gigabit LAN port, a reset button, optional AC power input, and a power button.

The ceiling/wall mounting kit, Ethernet cable, Quick Start Guide, and Product CD are included with the unit. The AC adapter and a PoE injector are sold separately.

On a side, you'll find the ports: two Gigabit LAN ports (one with PoE support), console port for debugging, a reset button, and the optional AC power input.

The default IP configuration for this unit is DHCP, so after plugging it in for the first time you must find the assigned IP address. Other than looking at your router or switch status, you can download their FindIT tool or use some other discovery tool. Once you access the web-based configuration screen you're presented with a setup wizard that helps you quickly configure the main settings: IP details, Single Point Setup, time, password, wireless radios, and captive portal for guest authentication.

We found the setup wizard, installation, and configuration processes to be straightforward. Single Point Setup is Cisco's name for their central controller-less access point management solution. You can create a cluster on one access point and then join up to seven more access points to that cluster and they'll inherit the same configuration settings, with a few exceptions, such as manually selected channels. Though you must bring up the web-based configuration screen for each access point, it's a very quick process to join them to an existing cluster.

No matter which access point you make configuration changes on when using Single Point Setup, the settings will automatically be propagated to all other access points in that same cluster. Of course, some settings are excluded from the synchronizing, such as IP and bridging settings. However, you cannot selectively disable the synchronization of certain settings like you can with the two other access points.

When navigating through the unit's web-based GUI, we found it supports wireless bridging and client bridge mode in addition to the traditional access point mode. It supports one management VLAN and up to 16 additional VLANs for use on up to 16 virtual SSIDs.

We also found some advanced features, such as band steering to help ensure capable clients connect to the typically less congested 5GHz band instead of 2.4GHz, load balancing to ensure access points aren't overloaded, and rogue access point detection to stay alert of any unauthorized access points in the area.

The unit also has captive portal functionality for authenticating guests via a local database or external RADIUS and/or requiring acceptance of the usage agreement. The access point also has a packet capture feature that you can use to remotely collect 802.11 packets received by the access point, useful for advanced troubleshooting.

On top of each page of the web-based GUI you can hit the Help link, which brings up the help documentation to that specific topic. We

found each feature and setting to be fairly well described.

D-Link DAP-2695

The D-Link DAP-2695 is designed for small to midsized businesses, as well as enterprise environments. Priced at $389.99, it's loaded with a three-stream (3x3) 5GHz radio, supporting theoretical data rates up to 1,300Mbps for 802.11ac and 450Mbps for 802.11n, and a separate radio for 2.4GHz. Their recommended user limit is 100 users per access point with 50 users per radio/band.

This D-Link unit has a gray and black plenum-rated metal chassis, which makes it the heaviest at about 2.5 pounds. However, its size is more comparable to the other two access points, measuring approximately 7.5 x 7.8 inches in length and width, and about 1.5 inches high. It sports six detachable dual-band antennas: three 4dBi antennas for 2.4 GHz and three 6dBi antennas for 5 GHz. On the top/front you have the normal LED status lights.

On a side, you'll find the ports: two Gigabit LAN ports (one with PoE support), console port for debugging, a reset button, and the optional AC power input.

Being pretty generous, D-Link includes both the AC power adapter and PoE injector along with a console cable. Like most other access points, it also comes with a mounting plate and hardware designed for wall mounting.

This D-Link unit comes from the factory set to a static IP, which requires you to temporary setup a computer with a static IP during the initial configuration. Additionally, once you log into the web-based configuration GUI, you won't find any wizard to help with the setup.

If you prefer, you can centrally manage up to 32 access points with D-Link's controller-less access point management solution, called AP Array. Set one access point to be the Master, one to be the Backup Master, and all others to Slave. The Backup Master and Slaves will inherent the settings of the Master. Like the Edimax unit, D-Link allows you to choose specific groups of settings to exclude from the synchronization. D-Link also provides the AP Manager II software that you can alternatively use to centrally manage this and other compatible access points.

After navigating the configuration screens, we found that the access point supports a few different modes in addition to the traditional access point: Wireless Distribution System (WDS) with Access Point, WDS/Bridge (No AP Broadcasting), and Wireless Client. It supports up to eight VLANs per band for implementing multiple SSIDs.

We also found some advanced features, such as band steering with configurable settings to help ensure capable clients connect to the typically less congested 5GHz band instead of 2.4GHz and load balancing to ensure access points aren't overloaded. Its web redirection features provides simple captive portal functionality. In addition to rogue access point detection, this unit provides ARP Spoofing Prevention to help protect against advanced hacking attempts and supports Microsoft's Network Access Protection (NAP) feature so network access can be stipulated upon client security and health requirements.

Like the Edimax access point, this unit has a built-in RADIUS server so you can easily utilize enterprise-class Wi-Fi security, but D-Link recommends a maximum of just 30 users.

Edimax WAP-1750

The Edimax WAP-1750 is designed for small to midsized businesses (SMB) and priced at $279.99. It's loaded with a three-stream (3x3) 5GHz radio, supporting theoretical data rates up to 1,300Mbps for 802.11ac and 450Mbps for 802.11n, and another three-stream (3x3) radio for 2.4GHz. Edimax says it's designed for high-density usage, supporting 100 simultaneous clients with 50 per band/radio.

On one side of the Edimax AP you'll find all the ports and buttons.

This Edimax unit has a white plastic housing and is the smallest and lightest at just over 7 inches square, less than 1.5 inches tall, and just over 1.2 pounds. The top/front has just a single LED light, showing the status of power to the unit. On one of the sides, it has three detachable external dual-band antennas, each with 2dBi of gain.

On an adjacent side from the antennas, you find all the ports and buttons: optional AC power input, two Gigabit LAN ports (one supporting PoE input and other with PoE output), USB port for system logs and saving/restoring settings, console port, reset button, WPS button, and a power switch. The Ethernet port with PoE output can be used to power other devices, like another access point or security camera.

Along with the usual Quick Install Guide, CD, and Ethernet cable, the unit comes with an AC adapter. It also includes a magnetic wall mount set.

When setting up the Edimax access point, you can either connect it to the network and it will get an IP via DHCP or you can configure via it's default static IP using a computer. When you bring up the web-based configuration screen, you won't find a setup wizard. Despite having no on-screen help either, the GUI is relatively attractive and user-friendly.

Edimax's built-in access point controller functionally is called the Network Management Suite (NMS), which allows you to centrally manage up to eight access points. Once NMS is enabled, you're presented with a modified web-based GUI on the access point that's set as the controller. By default, any new additional access points you plug into the network will automatically join the NMS as a slave and inherit the settings defined by the controller. Like the D-Link access point, you can optionally override select settings of certain access points.

In addition to the regular access point mode, this Edimax unit supports WDS with or without the access point functionality running concurrently. It supports up to 32 SSIDs, 16 for each band. The access point also offers a simple load

balancing feature and rogue access point detection. Like the D-Link access point, this unit has a built-in RADIUS server so you can easily utilize enterprise-class Wi-Fi security. However, the Edimax unit supports up to 256 user accounts. Another simple yet potentially very useful feature is its built-in beeper so you can make access points sound from the web GUI and physically locate them in the building.

Unlike the two other units, this access point does not support any band steering functionality, but Edimax says that's coming in the next firmware update. Though there's a guest network feature, the access point doesn't do any captive portal or web redirection, but Edimax says that's in the next update as well.

How we tested 802.11ac Access Point performance

For the performance part of the testing, we used IxChariot to run throughput tests on the access points with three different clients:

- **ASUS PCE-AC66 Dual-band Wireless PCI-E Adapter** (three stream 802.11ac) connected inside the Windows 7 PC, using the provided antennas attached directly to the adapter on the back of the PC tower rather than using their base extender.
- **Netgear A6200** (two stream 802.11ac) plugged into a USB 2.0 port on the back of the same Windows 7 PC.
- **Samsung Galaxy S5** (two stream 802.11ac) Android phone sat on top of the same PC during testing.

On the access points, we enabled WPA2/AES security and 80 MHz channel-width support, and set the 5Ghz channel to 153. All wired connections between the access points, wireless controllers, and testing endpoints were made via Gigabit Ethernet ports with CAT-6 cables. These connections were all tested and confirmed to be running near Gigabit speeds. During the testing, the distance between the access points and clients was about 25 feet with one wall and a closet partially blocking the line of sight (both made of drywall material).

We ran the tests with the IxChariot High_Performance_Throughput.scr script for one minute with each client individually in the 5GHz band. It simultaneously tested both the TCP uplink (client to access point) and downlink (access point to client), which I add to show the total simultaneous throughput. We ran each access point/client test three times and recorded the average and maximum throughput for each.

The Edimax unit came out on top with an average throughput rate of 242.8 Mbps, D-Link came in second with 235.4 Mbps, and Cisco last at 173.6 Mbps. ■

This chart shows average and maximum throughput in Mbps for each access point connecting via each of our three client devices.

	Edimax WAP-1750		D-Link DAP-2695		Cisco WAP371	
	AVERAGE	MAX	AVERAGE	MAX	AVERAGE	MAX
ASUS PCE-AC66	244.8	392.9	246.2	407.9	190.3	300.1
Netgear A6200	196.5	316.8	211.2	302.8	145.7	242.8
Galaxy S5	287.3	437.1	249.0	412.8	184.9	291.7

BY DAVID STROM

CHECKPOINT, WATCHGUARD EARN TOP SPOTS IN UTM SHOOTOUT

When it comes to unified threat management appliances aimed at the SMB market, vendors are finding a way to fit additional security features into smaller and more powerful appliances.

In 2013, we looked at nine UTMs. This time around we reviewed six products: the Calyptix AccessEnforcer AE800, Check Point Software's 620, Dell/Sonicwall's NSA 220 Wireless-N, Fortinet's FortiWiFi-92D, Sophos' UTM SG125 and Watchguard Technologies' Firebox T10-W. (Cisco, Juniper and Netgear declined to participate.)

We observed several megatrends across all the units that we tested:

- **Small is beautiful. Boxes are getting smaller and more powerful.** You don't need a 19-inch rack-sized unit any longer unless you have the need for connecting to a lot of cables or to buy something bigger that is designed to support a very large network. Throughput and features have gone up as the size of the box has diminished, too.
- **Big-ticket firewall features are entering the SMB UTM space.** Even these smallest UTM models offer features that are often found in the largest of enterprise firewalls. Today's typical UTM box includes application awareness, APT screening, and real-time threat visualization tools. While most small businesses don't have skilled IT staffs to handle all of these features, they are still nice to have.
- **Cloud management tools are more prevalent.** Several vendors work with various add-on features to scan files for potential malware, or to off-load management features into the cloud. For example, WatchGuard works with Lastline's cloud-based anti-malware tools, Sophos and Fortinet have cloud-based tools too.
- **Mobile VPN clients now available.** The VPN features on these boxes used to be more of an afterthought, but most of the vendors have beefed up their remote access features. Most products now have more of a selection of VPN types. They also offer the ability to support the built-in or open source mobile IPsec VPN clients of the latest phone and tablet operating systems. That is good news if you want to craft your own mobile device management alternative solution to at least protect data in transit with a smartphone. However, getting phones to work with these boxes is still somewhat of a chore. A few UTM vendors, such as WatchGuard and Calyptix, have added their own tools, clients, or configuration files to make establishing mobile connections easier, while others support the OpenVPN mobile clients.
- **Better botnet containment.** Fighting botnets is a cat-and-mouse war of attrition, but several vendors, including CheckPoint and Dell, have added specific policies to try to better contain these nasty forms of malware.
- **Better enterprise wireless management tools.** WatchGuard, Fortinet, Dell and Sophos all have beefed up their wireless management

ScoreCard

	Calyptix	Check Point Software	Dell/ Sonicwall	Fortinet	Sophos	WatchGuard
Installation	3.5	5	3.5	3	3	5
Features	3.5	4.5	4	4.5	4	4.5
Value	3.5	5	3	4	4	5
Total	3.5	4.8	3.5	3.8	3.7	4.8

SCORING KEY › 5: Exceptional, 4: Very Good, 3: Average, 2: Below Average, 1: Consisitently Subpar

features so you can deploy multiple access points around your office and manage them centrally from a single set of screens.

Winners

All six of these units will do fine for securing small offices of 25 people, but CheckPoint and WatchGuard stand out as the top vendors in this review. They have solid features, great user interfaces, and coverage across the multiple security technologies that form the basis of what UTM means today. Both also offer relatively inexpensive boxes for small offices with low annual subscription fees.

The others, though, aren't all that far behind. Dell and Fortinet have very tired Web-based interfaces that are in need of a complete overhaul. Sophos has great features but its interface has gotten a bit unwieldy too. And Calyptix shows a lot of promise and has a great way to price its box that the others should follow.

Calyptix

We tested the AE-800, which comes with four wired Ethernet ports that can be arranged in various VLANs or as a single flat network running version 3.1.15. None of the Calyptix boxes come with wireless access points. That could be a plus if you are worried that you will inadvertently leave your network open to wireless exploits or a minus if you have to deal with buying an additional wireless access points.

Calyptix has the simplest pricing: You get everything they offer without having to purchase individual subscriptions for particular features or for a certain number of users, and it also includes unlimited business hour phone support. If you have relatively modest needs (meaning don't have a lot of exacting security requirements) and are on a budget, this might be the right box for you.

We found that Calyptix has the least intuitive web UI, with a complex series of menu buttons across the top and left-hand sides, and the UI itself seems somewhat old-fashioned and a bit cryptic. They do get kudos for providing hotlinks to help texts for further explanations of their configuration settings though. Graphical elements are sparse: most menus are fairly text-heavy.

The Security menu is divided into four sections: Network, Web, Email and Instant Messaging. The latter is just a simple radio button to block traffic with each of the major IM protocols. Again, if you want more subtle controls, you will need to look elsewhere. Web filtering can white/black list particular URLs, and there is a place to test whether a domain will be blocked by your

settings. You can also block particular file types from entering your network through users' web browsers, such as PDFs or Word files, with a few simple menu selections.

The AE-800 does support load balancing to multiple WAN connections, but getting that setup will require some effort at navigating several menus to prioritize outbound traffic and set up firewall rules accordingly. Recent updates to their firmware include more accurate and faster antivirus scanning. Another nice feature is its best practices analyzer: it will look over all your settings and suggest ways to improve them.

VPN support is somewhat limited, but has an interesting usability feature. Most other vendors have a long list of files that describe particular client software versions. Calyptix puts all of its VPN client tools and configuration settings into one ZIP file, and you generate this file for each specific user. This is done using the web UI.

Currently, their VPN supports only IPsec and passthrough PPTP connections using OpenVPN for Windows, OS X and iOS. It also uses FEAT VPN for Android v2.1 or later devices. You'll want to review carefully the setup instructions that are included as part of the ZIP file, because of the several steps involved. But at least they put all the information together in one place.

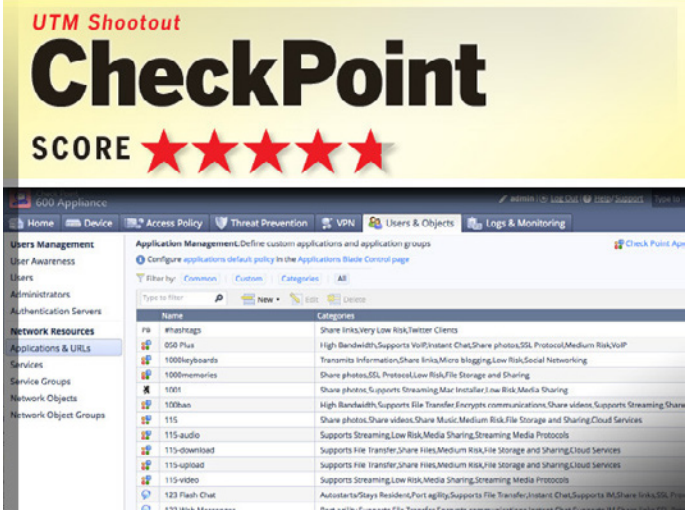
One downside is that only the administrator has rights to the entire box, meaning if you want to have someone else have partial rights you can't. Delegation of sub-admin rights is expected in an upcoming release. Another is that Web traffic doesn't go through the anti-virus scanner, but can be filtered by URL or content.

Reports can be scheduled on a daily, weekly or monthly basis, and can be sent via email or just collected in the unit's own archive. The first year's price for our unit was $999, with subsequent years costing $449. While not the least expensive, this is close to the bottom.

CheckPoint

When we looked at UTM devices in 2013, CheckPoint was far and away the best product. While it still has strong features, the others, in particular WatchGuard, are catching up. We tested an early version of the 620, which comes with eight wired Ethernet ports that can be arranged in various VLANs or as a single flat network and running vR77 of firmware. It features support up to four different wireless SSIDs.

CheckPoint has been our favorite in terms of ease of initial setup and its user interface is still the best by far. Commands are intuitively laid out, there is ample use of graphical elements and just by clicking on a couple of buttons you can easily create protective policies. For example,



adding a guest wireless network takes just a few mouse clicks and with an obvious link on the wireless settings screens. You can segregate wireless traffic for better protection with another mouse click.

Since we looked at its product in 2013, Check Point has added new security features such as anti-bot protection, which shares the same protective structure as anti-virus policies. They have also added mobile VPN clients to their mix of LL2P, SSL and IPsec VPNs. One nice feature is a link to the instructions on how to install and configure them from the Google Play or Apple iTunes Stores.

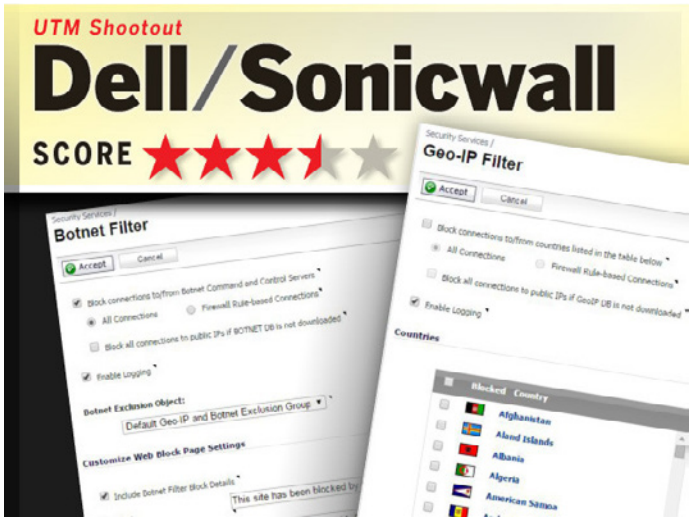
CheckPoint has beefed up its application controls, with more than 6,000 application policies, the most by far of any of the products we reviewed. You can quickly search through these and with a couple of clicks define a custom set of rules, such as 10 ways to regulate Facebook behavior across your network. Our only complaint is that they are tucked under the Users tab, making them initially hard to find. And with one click, you can place bandwidth limits on apps that can tend to hog it, like peer-to-peer networks and file sharing tools. This is one of the reasons why we continue to like what CheckPoint offers.

CheckPoint doesn't offer much in the way of reporting options, with overall summary reports for fixed time periods. But at least you can query its log files if you are trying to track down something suspicious.

One downside is that an administrator has full access rights to the entire box; you can only assign a secondary admin for read-only access.

CheckPoint has added a more capable cloud-managed security service for more granular management. This is useful for ISPs who want to centrally manage and support security policy management, firmware upgrades and automatic backups across multiple boxes. We briefly tested this feature.

Pricing is $598 for the wireless version that we tested, with a very low annual subscription fee of $100. This provides great value for the money.



Dell/Sonicwall

We tested the NSA 220 Wireless-N, which comes with seven wired Ethernet ports that can be arranged in various VLANs or as a single flat network and running v5.9 firmware. Dell continues to be in the middle of the pack: it isn't the most feature rich or have the most intuitive user interface, but it does deliver solid protection.

For example, others have more capable VPNs or offer more wireless options. If you used Sonicwalls before the Dell acquisition, you will find your way around their menu structure just fine. But if you are new to the brand, you will wish for

a new interface that is more usable, graphical, and simpler.

A case in point: Dell offers more than six different dashboards and at least as many setup wizards. These dashboards will show you in real time what is going on across your network, both from a bandwidth consumption as well as a threat analysis perspective. The wizards handle common tasks, such as setting up a switch port group or your wireless access. Navigating among all these choices can be daunting and take some time, which sort of defeats their purpose. On the other hand, once you run through the wizard, you probably don't need to ever see it again.

Another example: Dell doesn't offer the best support for VPNs, but they have widened their IPsec coverage somewhat and include mobile VPN clients for Android and iOS.

All Dell UTMs have integrated wireless access points, which exhibit this odd dichotomy. For example, you can schedule the times you want your wireless coverage to be active and you can manage an entire distributed network of wireless access points across your entire enterprise (which are both things just a few competitors have in their products), but configuring the wireless connection is somewhat cumbersome, requiring you to step through a series of several menus. You can set up multiple SSIDs with different security and access profiles though.

Dell has had the ability to set up specialized sub-admin accounts for some time, so you can delegate particular management tasks or have administrators view configuration settings in read-only mode. This is also missing in a few competitors' products.

Dell has made several functional improvements in its UTM code in the past year, and most of them are under the covers: adding distributed DoS flood and botnet protection, improving IPv6 support, allowing deep packet inspection with no limits on file sizes and adding bandwidth management on a per user or per IP address basis to identify and eliminate network hogs.

Another new feature is the ability to detect rogue access points so you can get a handle on who might be leaking data. They have included this as part of its intrusion detection screens. Several others have this feature, including Fortinet and Watchguard. Dell has also enhanced the cloud-based antivirus scanner to get the latest updates via an online repository. Finally, they have beefed up their real-time network traffic analysis so you can see which applications are active across your network and then add firewall rules to manage their use.

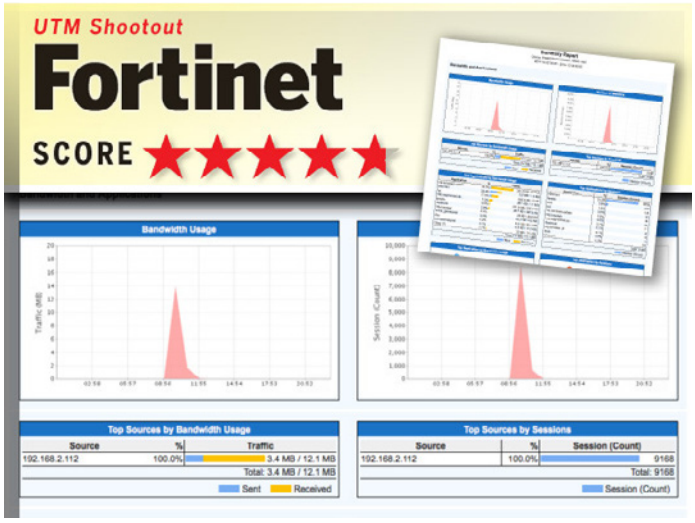
Pricing for the Dell is high, at an initial cost of $1,860, but a more reasonable recurring cost of $615 after the first year.

Fortinet

We tested the 92-D, which comes with 14 wired Ethernet ports that can be arranged in various VLANs or as a single flat network and includes four PoE ports and running v5.2.2 firmware.

Fortinet has always had a broad range of impressive features, they just aren't packaged very well. They are trying to make their Web user interface easier to navigate, but it still seems somewhat behind the times. There is only one setup wizard, and this can be run from the Web interface or via a special Windows or Mac configuration client with a USB connection to the box.

There is also a very meek attempt at a graphical interface for the feature selection, and they



have reorganized where particular control menus are located. This will confuse existing Fortinet users and newbies alike. As an example, their DOS and Instant Messaging screening options used to be part of the Web interface; now you have to use the command line for setting up both activities. Like Dell, it is time for a major interface overhaul.

However, they have added a few new things to their latest firmware release, including having the second broadest range of application signatures, at more than 3,400 separate rules. As an example, there are at least 60 of them concerning Facebook alone. CheckPoint has nearly double the total rule set but still what Fortinet has is impressive and both vendors are on par with application firewall specialty vendors such as Palo Alto Networks. You can add a signature to any firewall policy with just a few screens.

Fortinet also offers a primitive data loss prevention monitor, with checks on Social Security and credit card numbers only, although you can add a custom fingerprint to their process. The unit's Wi-Fi comes with two radios that can be set separately with different access rules. If you want more you'll have to purchase a separate wireless access point. This isn't as capable as some of the other vendors. It comes with built-in two-factor authentication using hardware tokens, email or SMS. And like Dell, it has support for a wide variety of sub-admin profiles. There are now more than a dozen configurations, and all can be set at read only or read/write access.

It also augments its anti-malware scanning by using a cloud-based sandbox. If you enable this option, files can be tested there as part of your protection policies. This is similar to how both WatchGuard and Sophos handle this. Speaking of the cloud, you can also store configurations there to provision multiple boxes, which is similar to how Check-Point uses its cloud management tool.

Fortinet's support for both SSL and IPsec VPNs is also middle of the pack. If you make use of their FortiClient software, you get both end-point antivirus protection and a VPN included in the package.

Pricing is $1,745 for the initial purchase with $584 a year for subscription renewals.

Sophos

We tested three boxes from Sophos: the SG125 that provides the basic UTM functionality, a wireless access point (AP15) and a Remote Ethernet Device (RED 10) that has some unique remote access features. Sophos actually has two UTM lines: the SG line that it originally acquired from Astaro (and which we tested using a slightly earlier firmware version last year)

and another line that they recently acquired from Cyberroam. Sophos is in the process of integrating some of Cyberroam's features into a subsequent release in 2015. Since they sent us the SG125, they now offer models with integrated wireless access points in them that carry a "w" suffix, such as the SG125w.

We tested version 9.3 of the UTM firmware. It includes some advanced features that distinguish the unit, including web server reverse proxy protection and the beginnings of APT protection. Also new is the ability to enforce web traffic policies on encrypted connections without the need to decrypt the actual traffic.

Both the general and wireless Sophos configuration took a bit longer to understand. We actually got our unit into some unworkable state and had to reinstall its firmware. Like most of these units, wireless connections can be segregated into their own VLAN, or combined with the general wired traffic. Multiple SSIDs can be created on the same access point for a separate guest network for example. Understanding the menus that provide this flexibility took some careful study, more so than the other units.

One nice default is that Sophos will send any file to be first analyzed with its cloud-based sandbox. There is nothing for the user to do; it is part of their scanning engine. Another advanced feature is the ability to support two-factor user authentication, there are a number of ways to set this up. Finally, it offers a nice change log that shows you all the various configuration options you have done as an administrator: we wish other boxes would offer this feature.

Sophos has improved its applications control, and while it is not as capable as Fortinet's, it can be easily accessed through the network flow monitor or by setting up an explicit policy on one of more than 1,200 behavior rules. For example, for Facebook there are 10 different rules.

Sophos VPN clients include support for both OpenVPN (include the iOS and Android clients) and Cisco VPN clients. One nice feature is being able to quickly access your Amazon-based virtual private cloud by either downloading the configuration file from Amazon or uploading this information from the UTM box. And for the easiest VPN access, there is the Remote Ethernet Device, a separate box that attaches to your remote network. You set up its identity on the UTM and it makes the connection easily.

Like Fortinet, Sophos has its own endpoint protection client called Live. It only works to protect Windows endpoints.

There are lots of reports that can be archived and accessed from Web UI, including a daily "executive report" that contains network usage, top destinations and clients, The reports failed

to disclose our BitTorrent activity, but that may be due to our error in setting up the correct policy.

Pricing was $1,280 for the initial purchase, with second and subsequent years costing $364 for annual subscriptions.

WatchGuard

We tested the T-10-W, which comes with three wired Ethernet ports that can be arranged in various VLANs or as a single flat network. WatchGuard has always had a mixture of Web, Windows and command line management interfaces. What is changing in the past year is which features are available under each interface, with the Web receiving some much-needed attention.

In October 2013 the company announced an upgraded tool called Dimension that carries several new features and is available with any UTM appliance running at least version 11.8 (we tested v 11.9.3). Dimension is a new real-time visualization tool that can be used to quickly identify emerging threats and network usage trends. Dimension is packaged as a virtual machine and is downloaded for free from the WatchGuard support website. It replaces the log servers that were difficult to interpret and search. Setting up Dimension is easy: you just point the log server from your UTM box to the appropriate IP address of your Dimension server, and it begins collecting information automatically. The company is in the process of taking some of the features from Dimension and moving them over to the web interface for several of their UTM appliances, including the T-10-W.

Here are some of the more interesting newer features:

- **Active threat map**, shows by location where identified threats originate by geo-locating their IP addresses. IT managers can use this information to block particular geographic access to their networks, or investigate potential oddities such as users from outside a particular state or city.
- **FireWatch** (which is also available through the web interface) shows you the most popular destination domains and most active users, along with other information in near-real time in a nice graphical area plot diagram. IT managers can use this information to tune their firewall rules and policies.
- **A variety of reports can be now emailed** to recipients from within the Dimension interface.
- **Executive dashboards** that summarize network activity and threats experienced in graphical form. Some of this information is available from the Web UI as well.

Even though the T-10-W is a small box, it has some solid management features that are found in larger UTMs and corporate firewalls. For example, you can set up to three different SSIDs using the built-in wireless access point and manage other access points that are external to the box. You can also segment the wireless traffic by specific firewall policies, so you could for example set up a guest network for visitors to your office.

There are some solid firewall features too: it comes with the ability to handle advanced persistent threats (APT) and data loss prevention situations. To get APT, you have to pass traffic through a proxy, then through the antivirus engine, and then to the APT routine. That takes some effort to setup. One benefit is that it works in conjunction with Lastline's cloud-based sandbox routine to determine if any malware has infected your system. Like Sophos, there isn't much to set this up, it is just part of the malware scanning process.

One other noteworthy item is the number of custom application behavior controls has been significantly beefed up: there are more than 2,000 behavior profiles that you can incorporate into protection policies. For example, there are 10 different Facebook profiles, so like Sophos and Fortinet, you can restrict traffic based on whether it is a Facebook game, or message, or Wall update. While not as numerous as Fortinet or CheckPoint, it is still impressive.

WatchGuard has excellent VPN support for L2TP, SSL (using OpenVPN) and IPsec VPN types. For IPsec you can use its own mobile VPN clients, the Cisco VPN clients that are built into Mac OS X or those from Shrew Soft. You set up a configuration using the Web or Windows management interface and then send that configuration file to the particular mobile device that you want to grant access. The mobile VPN clients support iOS v5 and higher, and Android v4 or higher.

Pricing was $630 for the initial purchase, with second and subsequent year subscriptions at $135 annually. This represents great value for the money.

How we tested UTM appliances

We connected each box to our small office DSL router and tried out the various Web and (in some cases) Windows-based management interfaces. We set up clients on various Windows 7 and 8 and Mac OS X machines as well as several iPhones of varying vintages. We assumed these devices will be placed on networks without any central Active Directory or RADIUS servers and added user accounts and set up security groups manually.

Once a box was connected, we updated the firmware and licensed individual software modules on each box, and then set up each UTM with WAN and LAN interfaces to operate with DHCP addresses whenever possible to remove the headache of managing IP subnets. We looked at what it would take to create a more restrictive policy for guest workers, as one example, and to see how to automatically block incoming threats. We added particular policies for sample users and performed other common tasks.

We examined packet captures across each box to see if firewall rules and other security policies were operating correctly. We also tried out various VPN and remote access connections from outside our office network to verify these features.

We evaluated the units based on these three criteria: installation, features, and overall value.

For installation, we reviewed the basic setup of the various network interfaces, users, and licenses. These products should be geared

towards smaller networks, with limited IT expertise and time to administer them. We looked at how much time was needed to set them up and configure properly.

When it came to examining features, we looked at the ability to manage and monitor the box remotely, set up new security policies, and review reports. We also looked at how well the basic five security modules integrate with each other, and what kind of workflow is needed to implement its protective features.

Finally, to assess value, we accounted for the overall first year purchase price plus the cost of any support and software licenses.

A note on throughput

We didn't measure throughput – instead we reported in the comparison table the data that we got from the various vendors. Since we didn't independently verify these claims, we suggest that you take the throughput numbers with several helpings of salt. All UTM boxes will bog down as you turn on more of their features, particularly the VPNs and the IDS that take more processing horsepower. The good news is that the ASICs inside even the lower-end boxes that we tested are getting better all the time, and that combined with offloading tasks to the cloud means that these products can handle more packet processing than ever before. ■

David Strom is the founding editor-in-chief of Network Computing magazine and has written thousands of magazine articles and two books on various IT and networking topics. His blog can be found at strominator.com and you can follow him on Twitter @dstrom. He lives in St. Louis.

FeaturesTable

Vendor/ Product	Price: 1st year (HARDWARE/SUPPORT) 2ND YEAR (SUPPORT, LICENSE FEES)	Wired GigE LAN Ports	VPN Support /Clients Available	Additional Modules	Throughput (BASED ON VENDOR-SUPPLIED DATA)
Calyptix AccessEnforcer AE800	$999/ $449	4	Fair/ Excellent	N/ A	100 Mbps
CheckPoint Software 620	$598/ $100	8	Excellent/ Excellent	Anti-botnet	1.5 Gbps (FW) 220 Mbps (VPN)
Dell/Sonicwall NSA 220 Wireless-N	$1,860/ $615	7	Good/ Good	Cloud AV	110 Mbps
Fortinet FortiWiFi-92D	$1,745/ $584	14	Good/ Good	Sandbox AV, DLP	700 Mbps
Sophos SG 125	$1,280/ $364	7	Good/ Excellent	3 boxes, including Sandbox	165 Mbps
WatchGuard Technologies Firebox T10-W	$630/ $135	3	Excellent/ Excellent	APT, DLP, Sandbox	55 Mbps