Tech Outlook

PROSYS
A PIVOT COMPANY

November 2016

THIN CLIENTS ON THE ROAD

Mobile thin clients provide the productivity benefits of mobility plus tighter control over enterprise data.

The rise of the mobile workforce began at the grass-roots level, as employees started using their personal mobile devices for work-related tasks. Organizations appreciated the productivity boost gained when employees could work from virtually any location. However, IT departments worried about the risk of malware and the loss of sensitive information.

Bring-your-own-device (BYOD) programs attempted to allay these concerns, with policies, procedures and management tools aimed at securing mobile devices and protecting applications and data. They have only been nominally successful. A recent IDC survey found that security issues and cost overruns are persistent problems even as organizations plan to increase their spending on mobility.

These challenges are prompting organizations to consider alternatives to BYOD. Nearly three-quarters of U.S. enterprises offer a choose-your-own-device (CYOD) program, or plan to do so in the coming year.

continued on page 2

continued from page 1

CYOD allows employees to select from a limited menu of approved devices that have been preconfigured with security controls. The employee buys the device but the company retains legal rights to the data. In a third model called COPE (corporate owned, personally enabled), the company supplies employees with devices that can be used for personal as well as business functions.

"None of these deployment options is completely satisfactory," said Ariel Valdes, Lead Data Center Architect, ProSys. "While CYOD and COPE give organizations greater control over the security of the device, data is still going outside the firewall and employees are potentially connecting to insecure networks. This often creates an unacceptable level of risk, particularly in highly regulated industries.

"That's why mobile thin clients are an increasingly attractive alternative to smartphones and tablets. They allow workers to access virtual desktops from any location while tightly restricting other uses."

> **Older thin clients had somewhat limited uses, but newer offerings have the processing power to support graphics-intensive applications and deliver a great user experience."**

Old Concept, New Approach

Thin clients have been around for decades, offering an alternative to full-blown PCs for users who don't need local processing power. Lightweight computers that emphasize network access and graphics processing, thin clients can dramatically reduce desktop management costs while increasing security and data protection.

"Desktop PCs require a lot of care and feeding, including hardware and software updates, security patches and backups," said Valdes. "Thin clients require none of those things, so they have a much lower cost of ownership — studies have shown that thin clients can reduce desktop support costs by as much as 80 percent compared to 'fat client' PCs. Security is enhanced because users can't make configuration changes or inadvertently introduce security threats.

"Older thin clients had somewhat limited uses, but newer offerings have the processing power to support graphics-intensive applications and deliver a great user experience. Organizations are also taking a fresh look at thin clients as they face the need to upgrade their Windows 7 PCs."

Originally, thin clients were conceived as an alternative to the "dumb terminals" used to access applications on mainframes. Today, they're more commonly associated with virtual desktop infrastructure (VDI), which allows organizations to host desktop environments within the data center. They are also increasingly used to access cloud-based applications and services.

"Mobile thin clients put these features and benefits in a highly portable form factor," said Valdes. "The concept is not new — for years, vendors have offered mobile thin clients that were essentially stripped-down laptops. But as mobile devices have become lighter and more powerful, so have mobile thin clients, with numerous options now available to support a wide range of use cases."

Power and Portability

Dell recently announced its redesigned mobile thin client portfolio, including the Dell Latitude E7270 and Latitude 3460. The solutions integrate the manageability, performance and security of Wyse thin clients with the enterprise-class capabilities of Dell's Latitude laptops and ultrabooks.

The Dell Latitude E7270 is designed to meet the exacting needs of power users, with an Intel 6th Generation Core i5 processor, four-cell battery and 12.5-inch Full HD (1920 x 1080) antiglare display. The Latitude 3460 provides an enterprise-class mobile experience for a broad range of use cases, with an Intel Celeron 3215U processor and a 14-inch HD (1366 x 768) antiglare display. Both feature a wide range of connectivity options and ports, including USB 3.0, HDMI, gigabit Ethernet, and WI-Fi and Bluetooth options. They also provide extended battery life for all-day productivity.

"Dell's new mobile thin clients are based upon Windows Embedded Standard 7 64-bit for a familiar local Windows experience," Valdes said. "They support all VDI protocols, and can connect to all of the major brokers including Citrix XenDesktop, Microsoft Hyper-V and VMware Horizon. They are also easy to deploy and manage, with flexible configuration and management via Wyse Device Manager or Microsoft System Center Configuration Manager. IT managers can easily scale administration from just a few to tens of thousands of mobile thin clients to meet growing user demand."

Mobile thin clients are ideal for a range of industries including finance, healthcare, government, manufacturing, and energy and exploration. They enable remote and mobile workers to securely access applications and data, while ensuring the security, manageability and centralized control provided by a virtual desktop environment.

News Briefs

Industrial IoT Security Outlined

The Industrial Internet Consortium (IIC), the global organization formed to accelerate adoption of the Industrial Internet of Things (IIoT), has announced the development of a common security framework that addresses security issues in IIoT systems. The Industrial Internet Security Framework (IISF) defines risk, assessments, threats, metrics and performance indicators to help business managers protect their organizations.

"Today, many industrial systems simply do not have adequate security in place," said Dr. Richard Soley, executive director, IIC. "The level of security found in the consumer Internet just won't do for the Industrial Internet."

The framework document, available free of charge, goes into technical detail about recommended implementations, though it stops short of recommending specific products. The long-term goal is to make sure security is an integral part of every IIoT system and implementation.

The framework is intended to help business managers within industrial organizations make informed decisions based on well-designed risk assessments. From a functional perspective, the framework separates security evaluation into endpoint, communications, monitoring and configuration building blocks with subdivisions for each one. Each perspective offers implementation best practices.

More IT Workloads Running in Cloud

Forty-one percent of all enterprise workloads are currently running in some type of public or private cloud, and that number is expected to rise to 60 percent by mid-2018, according to a new report from 451 Research. Based on interviews with more than 38,000 senior IT buyers and enterprise technology executives, the report anticipates strong growth in both the Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) deployment models.

The research firm says that enterprises are currently most likely to use on-premises private cloud and SaaS, with each model accounting for 14 percent of all applications. While usage of on-premises private cloud is expected to remain flat over the next two years, SaaS growth is expected to reach 23 percent of all enterprise workloads in that time frame.

Although only 6 percent of enterprise workloads currently run on IaaS, this model is likely to see the highest growth over the next two years, with usage predicted to double to 12 percent of workloads.

"The predicted doubling of IaaS usage is the highest growth expectation for any type of cloud and points to significant revenue potential for vendors in this space," said Andrew Reichman, Research Director of 451 Research. "Because cloud delivers increasing agility and flexibility to better fit ever-changing business needs, IaaS and SaaS allow organizations to focus their efforts on their business, rather than on maintaining costly and complex data centers and infrastructure. If used properly, it has the potential to dramatically improve efficiency and results of business technology usage."

Tech Outlook

Editorial Correspondence:
10221 E. 61st Street
Tulsa, OK 74133
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosysis.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosysis.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosysis.com

The Carolinas
Toll-Free: 888-337-2626
chash@prosysis.com

Indianapolis, IN
Phone: 317-688-1283
Bill.sanders@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
info@prosysis.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
pmadden@prosysis.com

Mexico City
Phone: +52 (55) 3601 3755
pmadden@prosysis.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
midatlantic@prosysis.com

Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
pmadden@prosysis.com

New England
Toll Free: 800-634-2588 ext 1
newengland@prosysis.com

Seattle, WA
Phone: 425-939-0342
sballantyne@prosysis.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

WLAN Evolution

Network design focus shifts from coverage to capacity.

Anthropologists say there was no appreciable improvement in the design of stone hand axes for some 60,000 generations — a period sometimes referred to as "the million years of boredom." However, the emergence of metallurgy enabled new methods of toolmaking, sparked the transition from the Stone Age to the Metal Age, and inspired profound social evolution.

Design is by nature an evolutionary craft, a continual effort to develop more effective solutions to the challenges we encounter. Wireless networking is currently undergoing one of these design evolutions. As Wi-Fi has grown from a "nice-to-have" technology to the essential enabler of the connected enterprise, organizations must rethink their approach to wireless LAN design.

Until recently, Wi-Fi has been deployed with an eye toward coverage of a physical space. Coverage-oriented design focuses on the placement of access points (APs) to provide adequate signal strength and ensure there are no dead spots in the area. The approach was meant to provide service to limited numbers of wireless users, using a limited number of devices and requiring limited bandwidth.

Those limits have vanished.

The proliferation of smarter, more portable devices combined with advanced mobile application platforms have fundamentally altered the requirements for WLAN design. Organizations need to support more wireless users, devices and traffic than ever before — and they must be prepared for continued growth for the foreseeable future. Industry analysts anticipate that wireless data traffic will soon surpass that moving over wired networks.

"Recognizing the critical role that WLAN plays in IT's mobility and digital initiatives, enterprises are committing to WLAN upgrades and refreshes," said Nolan Greene, senior research analyst, Network Infrastructure at IDC. "Even as global economic indicators are mixed, IDC believes that enterprises will continue to invest in robust WLAN infrastructure in order to compete effectively in the digital economy."

More Can Be Less

As wireless demands continue to increase, the focus of Wi-Fi network design is shifting from coverage to capacity. In other words, simply providing basic coverage in a defined service area is no longer sufficient. Organizations need to ensure that the Wi-

Fi network supports the current and future capacity and performance levels required of an increasingly mobile workforce.

It might seem like a simple matter of adding more APs — after all, the closer a wireless client is to an AP, the better the data rate. It stands to reason that more APs will increase the raw capacity of the WLAN by closing the distance between clients and APs.

However, it isn't that simple. Too many APs will actually degrade WLAN performance by creating oversaturation. Wireless clients can become confused trying to access multiple APs with similar signal strength. The effect is similar to when a car radio picks up signals from multiple radio stations broadcasting on similar frequencies.

One way to avoid this issue is with band-steering technologies that reduce traffic on the crowded 2.4GHz band by shifting capable devices to the less-congested 5GHz band. This technique, in combination with directional antennas, high minimum bit rates and low power settings, can provide a good deal of capacity while limiting interference.

High-capacity Wi-Fi planning must also account for variables such as overprovisioning for variations in traffic patterns, optimal use of the wireless spectrum, load balancing, Quality of Service and other factors. This involves careful planning in order to integrate the right number of APs to handle the increased usage without introducing interference.

Professional Planning

A technology-neutral managed network services provider will typically begin the design process by interviewing stakeholders to learn the types and numbers of devices and applications that are being used. This helps in determining the aggregate bandwidth required in the coverage area.

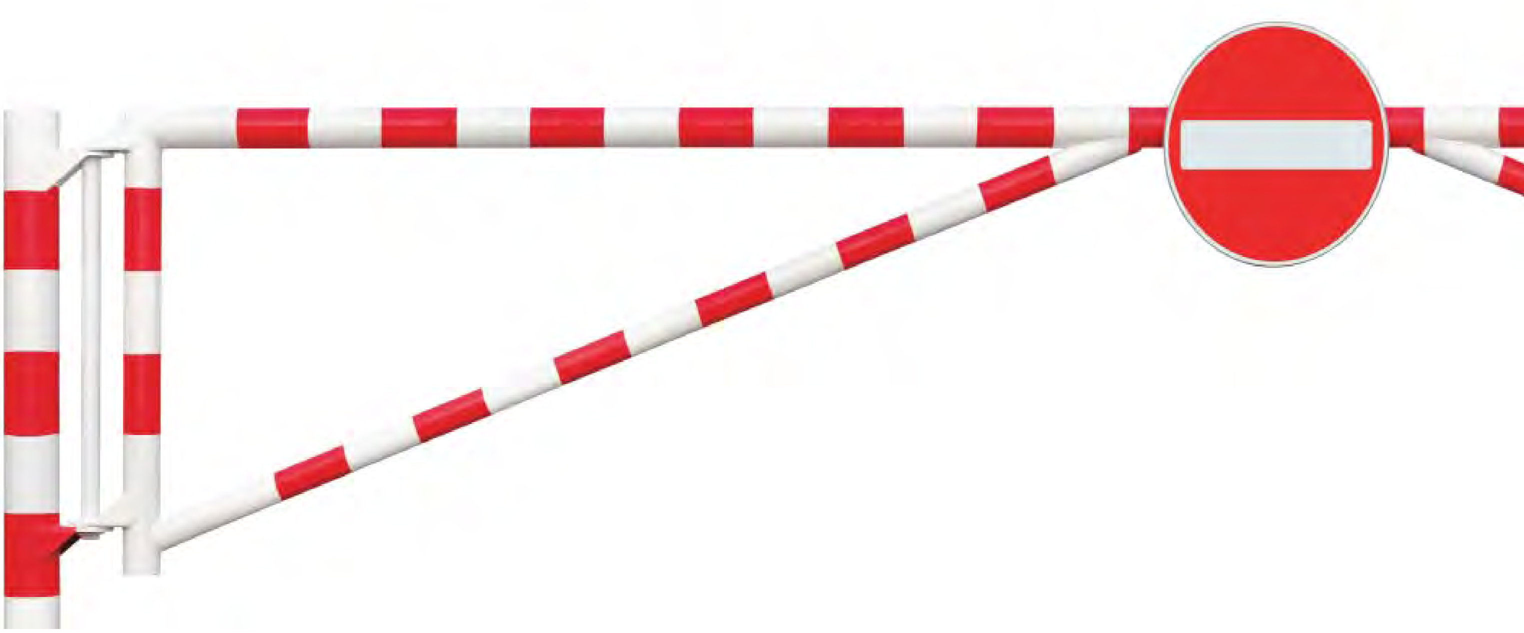
The next step is an onsite survey, which usually involves physically walking around the site and measuring signal strength in various locations in order to build a coverage map. A sweep with a spectrum analyzer will also identify any sources of radiofrequency interference.

Software-driven predictive site surveys now provide an even clearer picture by creating 3-D models of the environment with network simulations and heat maps that give a visual representation of anticipated signal strength and application throughput. A major benefit of predictive modeling is the ability to quickly simulate multiple deployment scenarios and narrow the possibilities to the most-promising alternatives.

Coverage-based WLAN designs were meant to accommodate the occasional wireless user, but they no longer meet modern demands. There are now more mobile devices in the world than there are people, and wireless networks carry more than 100,000 times the traffic they did in 2008. Wireless directly impacts economic growth and productivity, and businesses now rely upon devices and services that didn't even exist 10 years ago. Evolving design principles focused on capacity requirements can help ensure that organizations aren't stuck with archaic WLAN performance.

BORDERPATROL

Enterprise session border controllers help ensure security, interoperability at the edges of communications networks.



The session border controller (SBC) is one of the bedrock technologies in IP communications, acting as a gatekeeper between customer and carrier networks in order to implement security and regulate traffic. However, it has traditionally been a one-sided relationship, with SBCs implemented almost exclusively by carriers on their side of the connection.

As the threat landscape evolves, organizations are rightfully becoming reluctant to depend entirely upon service providers to secure the network edge. This has led to steady growth in the market for customer-side SBC deployments, commonly known as enterprise SBCs (eSBCs). According to the technology market research firm Infonetics, eSBC revenues grew from just over $60 million in 2013 to $271 million in 2015, with the market expected to reach $422 million by 2018.

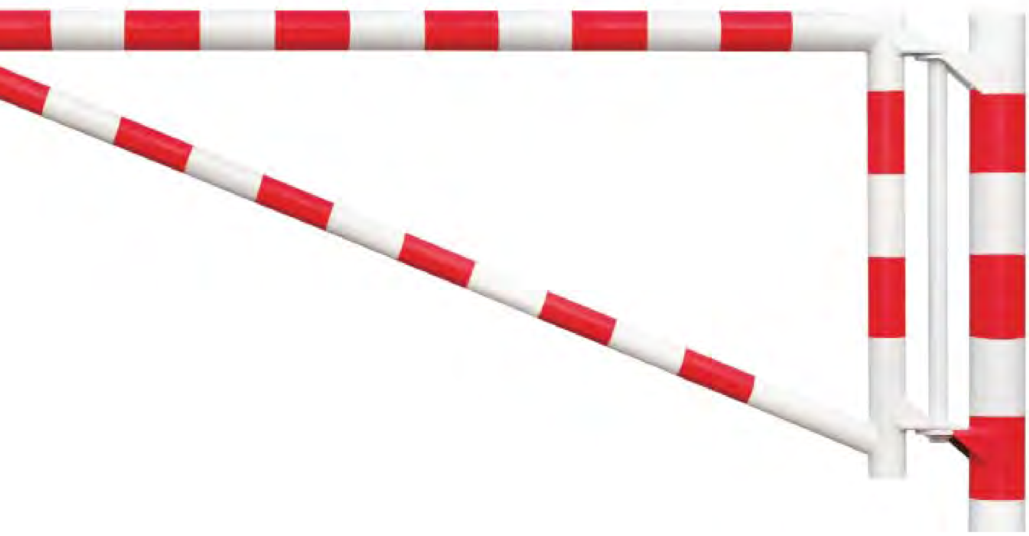
"The use of enterprise session border controllers is becoming more mainstream with the adoption of SIP (Session Initiation Protocol) trunking services, where SBCs are used as a border element between enterprise and service provider networks," said Diane Myers, principal analyst at Infonetics.

Traffic Control

There is a growing emphasis on customer-side protection as organizations of all shapes and sizes continue to adopt unified communications (UC) solutions in order to optimize processes, decrease operational costs, improve efficiency and increase productivity. While the benefits are compelling, UC can introduce a number of security and operational challenges. In a recent Dimensional Research survey commissioned by Dell, 77 percent of respondents said they have data security concerns with their UC solutions, and 55 percent report they spend time every week responding to UC quality issues.

Many challenges stem from the fact that IP-based communications platforms are inherently open, unlike traditional copper-based voice networks that are closed and therefore reasonably secure from outside threats. Voice, video and data traffic conveyed along the public Internet is potentially exposed to a wide range of threats.

Complicating matters is the fact that conventional IP networking components such as routers and firewalls are not designed to manage real-time communications and can cause latency problems for time-sensitive voice and video traffic. Interoperability issues at the network edge can create additional performance problems.



eSBCs help alleviate these concerns. Deployed as either dedicated hardware devices, software applications or virtualized network functions, eSBCs help secure the network edge, regulate traffic in and out of the network, and normalize signaling and media used in real-time communications.

Securing SIP

The best eSBCs are not merely repackaged versions of carrier-grade products, but are designed to be affordable, scalable and easy to manage and install. Many of the design characteristics are focused on securing voice communications through SIP trunks.

SIP is the standard signaling protocol used to establish voice and video connections in UC solutions running across a data network. A SIP trunk connects the IP-PBX to the traditional Public Switched Telephone Network (PSTN) over an Internet connection. However, there is significant risk with connecting the UC system with an IP connection. Because SIP packets are typically delivered in plain text, they can be attacked or manipulated by hackers.

The eSBC boosts security by serving as the connection between the UC infrastructure, the Internet and the SIP trunk. It terminates and re-originates each communications session, processing traffic in real time to identify incoming threats. It also offers deep packet inspection, policy enforcement and other security functionality, providing more control than an application-layer firewall.

Speaking the Language

Another key function of an eSBC is to act as a translator at the network edge. Since SIP was introduced in 1999, there has been constant development of new extensions to add features on top of the basic protocol — sometimes there can be multiple extensions that perform the same function, such as call forwarding or caller ID. As a result, SIP providers generally run customized versions of the protocol. An eSBC at the network edge provides protocol normalization to enable communication with multiple carriers.

An eSBC also must translate a wide range of the codecs that convert audio signals into compressed digital form. Early VoIP solutions used fairly standard sets of codecs, but carriers and service providers have since developed dozens of new codecs — some of which may not be supported at both ends of a communications session. With support for most codecs, eSBCs can normalize communications without any data loss or latency.

Such protocol translation and normalization is important for organizations that take an incremental approach to VoIP migration, enabling legacy and IP systems to coexist during the transition. The eSBC intercepts calls from the telecom provider and routes them to the appropriate system in a way that is seamless from the end-user's perspective.

Support for mobile devices in a UC environment is another factor in the growth of eSBC deployments. By delivering secure SIP communications for mobile devices, an eSBC eliminates the need for remote workers to dial into their network through a virtual private network (VPN) tunnel. This simplifies authentication and eliminates the performance overhead of establishing a VPN tunnel.

Organizations today need a workforce of employees who can stay connected to business communications while in the office or on the go. While the growth of mobile and UC platforms enable new levels of collaboration and productivity, technology conflicts can occur along the boundaries between wired, wireless and cellular networks. Enterprise session border controllers ease those conflicts by connecting disparate networks, mitigating security threats and ensuring reliable communications.

Secure Performance, Effortless Portability

Dell's new mobile thin clients are purpose-built for on-the-go professionals who require superior protection for the data and intellectual property. The Latitude E7270 and 3460 mobile thin clients are designed to securely deliver virtual desktops to mobile users. They incorporate Intel's quad- and dual-core processor technology that packs plenty of power to support a broad range of apps and use cases, with integrated graphics for a rich multimedia experience. These mobile thin clients deliver great value with a 14-inch or 12-inch Full HD anti-glare display and robust connectivity with plenty of ports.

Both models support a wide variety of virtual desktop brokers, including Citrix XenDesktop and VMware Horizon, and can connect to a broad range of peripherals and desktop / application virtualization environments using a fast, rich and familiar Windows user experience.

To learn more about how these devices make mobile cloud computing more secure and efficient than ever before, contact your ProSys representative.

PROSYS
A PIVOT COMPANY

www.prosysis.com 888-337-2626

DELL-08