



Corporate networks: Business 2.0 and beyond

SonicWALL® **ECLASS**

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™

The performance and security needs of corporate networks have evolved greatly in the last five years, driven by changing business and economic demands, different patterns of working and a continuous stream of new technologies. In this environment of 'Business 2.0', the network is the organization's vital beating heart, a strategic business tool used by companies to drive significant competitive advantage. But this central role also brings management, risk and security challenges. This brochure provides a management overview of what's changed and why. But more importantly, it shows why flexibility, visibility, agility and affordability are now the key factors in network decision-making.

From privilege to prerequisite

As with mobile phone networks two decades before, easy access to corporate networks has turned from being a 'nice but non-essential' for the privileged few, into an 'expected right' used by the majority of an organization's employees, wherever they choose to work. Capturing all of the resulting business benefits—whether it's faster, better decision-making or higher employee productivity—is IT management's enduring challenge. It's a complex challenge defined by trade-offs and conflicts, as we will see.

The quest for competitive advantage still remains important but the demand on today's corporate networks has moved beyond this high-level aim to something more fundamental—economic survival. Meanwhile, network security considerations have proliferated. Five years ago, almost all corporate data and applications were held on a centralized network with secure access controlled using the 'fortress approach'—a technological equivalent of a walled perimeter accessed via permitted entry points or 'gateways'. But this approach is increasingly seen as an inhibitor to today's agile business models.



The network as an enabler of strategy

The new network architecture is enabling business agility on a whole new level. A SonicWALL customer in Australia has been able to pursue a fast-paced merger and acquisition growth strategy that until recently would have seemed impossible. It uses SonicWALL's Aventail E-Class Secure Remote Access appliances to provide secure, remote access for acquired businesses to its corporate network wirelessly via the Internet. This cuts out the delay and expense of connecting via the fixed telephone network and means the company can begin to realize value from newly acquired businesses much faster than before.

Today's industry talk is of the 'dynamic perimeter', a very different realm in which applications and data are location independent, one where information flows securely across unconventional network boundaries and there is no distinction between internal and remote users. In this new network environment, data security issues include:

- Managing, controlling and securing access to high volumes of fast-moving, sensitive, de-centralized corporate data: the bigger the organization, the bigger the challenge
- Defining and achieving the right balance between security and speed: the agility trade-off
- Ensuring business units and the extended enterprise of suppliers and business partners meet corporate (or industry) compliance standards
- Threat mitigation, from the malware of increasingly organized and sophisticated criminals

Despite this, IT professionals must operate under the same, harsh economic realities as those in other business functions. Reducing operational expenses has become a fundamental concern. That means doing more with the same or less resources, and clearly demonstrating real business value in any additional resource requests. It also helps if you can show the total cost of ownership in demonstrating the wider business value of all existing IT assets.

And as if all this wasn't enough, IT professionals face other demands. They must adapt to the Web 2.0 world, help minimise their company's environmental impact and take on an increasingly strategic role; it is no longer enough to provide a reactive service to the business.

How networks are changing in response

Security, agility, productivity, and now, frugality; how are companies meeting these and other demands on their networks? One increasingly common approach is through server 'virtualization'. Most servers run at only a fraction of their capacity at any one time. Virtualization allows multiple, 'virtual PCs' and other hardware to run separately, using the capacity of fewer servers more intensively. In this way, companies reduce costs associated with rack space leasing and hardware maintenance but also energy costs and carbon footprints. It's not just about cost and carbon saving, though. Virtualization also permits agility. As a company's business levels ebb and flow, virtualization allows faster deployment of new servers and new or modified applications.

Cost and carbon-saving benefits are also partly behind the emergence of network security consolidation combined with 'virtualized' Unified Threat Management appliances. Consolidation also removes complexity from IT systems—rarely a bad thing—allowing greater visibility for decision making through simplified reporting. But the key attractions of such a strategy are the ease and low cost of scaling up security to meet changing business needs or rapidly evolving threats.

Some organizations are going further still as part of wider, 'lean computing' initiatives. They are drawn to the inherently more flexible, low up-front investment and pay-per-use models permitted by cloud computing and software-as-a-service providers. Developments such as these allow companies to abandon the high initial capital expense and lock-in of owning IT assets outright. Even those who haven't taken this step are sending resource-intensive IT tasks such as data backup or heavy-duty data processing to 'the cloud'.

Virtualization, cloud computing, consolidation, convergence—all are happening now. Deployed in unison, they allow corporate networks to be designed, operated and managed in a completely different way. The challenge for CIOs is to make this transition, maintaining high levels of security, while anticipating and adapting to the next wave of change.

Emerging trends and technologies

To do all of this requires IT to move away from being a service-driven cost center to become a value-added strategic partner. That means unshackling itself from some of the current resource-heavy service obligations such as helpdesks and user support. These services will shrink as companies increasingly deploy self-service and self-remediation. Moves like this will free up management time to better plan for the next step change, such as the likely rise in high bandwidth, unified communication.

Voice and data networks are already converging on a large scale as companies pursue the significant cost saving and productivity improvement opportunities. High-bandwidth unified communication may soon overtake e-mail traffic on the network, as businesses find new ways to harness existing and emerging Web 2.0 applications, and smart phone-equipped 'net generation' employees become the majority. Some are even predicting e-mail's demise entirely with the arrival of peer-to-peer applications, video chat and micro-blogging sites like Twitter. Should those predictions prove correct, this would be a significant moment in information technology's short history. The implications for network design, bandwidth capacity, security, service quality and productivity are likely to be equally significant. Web 2.0 applications and social media sites not only negatively impact productivity, they also devour bandwidth, putting them in competition with business-critical applications. IT must have the visibility to see to what's happening on the network at any given moment in order to prioritize network bandwidth usage. And being able to do that based on the application, type of service, content or user profile has changed from being an option into an essential.



Unintended consequences

Who would have thought a game of golf happening in one country would seriously disrupt hundreds of businesses on the other side of the world, effectively cutting off access to vital corporate information? Yet this is exactly what happened during Tiger Wood's closing victory in the 2008 US Open Golf Championship. Avid fans in their thousands, still at work in Europe, logged on to watch live, Web-streamed television coverage. Fortunately, users of SonicWALL's E-Class Network Security Appliances found they could quickly prioritize access to selective streaming applications, prioritizing network bandwidth to business-critical resources. In other companies, events took a different turn. Golf-loving employees effectively crippled their corporate networks, catching IT management on the back foot and leaving them with some explaining to do. It's a graphic example of how network resources can easily become overwhelmed without judicious deployment, and just one of the many management challenges arising from the new network architecture.

Implications for security

In the new, dynamic network architecture, remote corporate sites, customer sites and outsourcing partners all reside outside the traditional security perimeter, as do employees' mobile and wireless devices. The distinction between internal and external network user has disappeared. A further development is the concept of deploying enterprise-level network security and connectivity rapidly, as and when needed; the so-called 'virtual perimeter'. Both mean increased likelihood of security breaches. The answer is multiple layers of protection or a 'defense in depth' approach, to shield all of these elements, as well as the core/distributed networks and data centers themselves. Such an approach provides secure access to data and applications by users of devices beyond the perimeter, plus secure data flows across the perimeter.

Two other security issues for network managers to contend with are non-technological and arise from the economic downturn. Rising numbers of employee lay-offs requires extra levels of vigilance against the potentially destructive actions of disgruntled employees. And reduced headcounts in many companies has spawned a rise in short-term contractor and outsourcing use to plug shortfalls. Both require higher levels of data monitoring and preservation, plus the ability to rapidly deliver connectivity, security and data backup and recovery.

All this needs to be accomplished at a time when cybercrime continues to proliferate. Organizations can quickly find themselves under targeted attacks by accomplished criminals. Proactive, multi-layer security strategies must be implemented in order to provide the highest level of protection.

Summary

- Networks are evolving at a faster pace: drivers are technological, social, regulatory, macro and micro-economic, as companies seek to redeploy IT investments more intelligently
- A 'lean, green, frugal and fast' mindset has emerged and is shaping major corporate IT decisions
- Bandwidth demand is set to rise exponentially, requiring astute network management
- Security and compliance threats are proliferating, placing extra demands on CIOs
- Deploying the right network design and appliances can deliver real strategic advantage
- Low cost and high quality/speed/security are no longer mutually exclusive

Business 2.0 and beyond: SonicWALL's position

Since 1991, SonicWALL® network security and data protection solutions have kept customers ahead of ever-evolving threats and changing work practices. Today, SonicWALL offers a full range of enterprise-class cost-efficient solutions to defend, control and manage corporate networks. They cover: unified network security; secure remote access; Web and e-mail security; backup and recovery; policy and management. All of them permit and facilitate the deployment of cloud services, virtualization, consolidation and de-perimetered network approaches the new world demands. Find out more about SonicWALL's Enterprise Business Solutions by visiting www.sonicwall.com

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com



PROTECTION AT THE SPEED OF BUSINESS™