Network Management—From Reactive to Proactive Mode Using Centralized Management Tools
Network Management—From Reactive to Proactive Mode Using Centralized Management Tools

By Robert Whiteley and Matthew McKinley

This IT Briefing is based on a Stonesoft/TechTarget Webcast, “Network Management—From Reactive to Proactive Mode Using Centralized Management Tools.”

This TechTarget IT Briefing covers the following topics:
- Network Management Practices
- The Changing Role of Networking
  - New External Requirements and Pressures
  - Changing Network Operations Skills
  - Widening Network Skills Gap
  - Addressing These Challenges
- Network Management Tools
- Closing the Skills Gap
- Getting Started
- Managing Today’s Networks
  - Increased Network Infrastructure Complexity
  - Truly Distributed Networks
  - Rapidly Changing Regulatory Requirements
  - Ensuring Security and Resilient Connectivity
  - Turning Data into Intelligence
- The Maze of Network Management Options
  - The StoneGate Platform
- Recommendations
  - Determine the Right Place to Start
  - Choose the Best Partner
  - Establish the Most Important Metrics
- Common Questions
Network Management—From Reactive to Proactive Mode Using Centralized Management Tools

Network Management Practices

In many corporations, network management practices are out of date. New tools and approaches are needed. It is time for IT departments to change from reactive to proactive and become more vigorous in the process of network management. Many opportunities for improvement involve organizational redesign from a staffing perspective and the realignment of IT—networking in particular—with modern business demands. Centralized management tools enable people to be more efficient in supporting networking technologies throughout the business.

The first topic of discussion is the changing role of networking within business and the consequent change in the demands placed on networking professionals to implement new technologies and acquire new skills. The second topic concerns the ways in which management tools are helping IT departments address some of the key challenges facing network professionals. The third topic lays out the options for network management tools and explains Stonesoft’s product, StoneGate. The final topic consists of recommendations for getting started based on good practices in corporations with which Forrester has worked.

The Changing Role of Networking

Figure 1 illustrates how the network is now front and center for many of today’s IT initiatives and architectures.
architectures. Yet the network in its current form is actually under siege. IT consolidation initiatives are common, including the consolidation of servers, facilities, branches, and data centers. This activity increases the amount of network connectivity necessary for these more centralized consolidated assets. Content delivery, including voice, video, and rich media, is really impacting the wide area network. This may be directed toward consumers, customers, or business partners. Distributed applications, the move to Web 2.0, and programs such as SharePoint that really open up collaboration and extranet all have big network implications. Also, good old replication and backup are essential network activities as companies move to a more explicit IT-based way of working over distributed networks, especially when they try to meet new disaster recovery objectives. And finally, virtualization technology, server storage, desktop—all the different flavors of virtualization—drive changes in network requirements, because they are dependent on the network that connects people to all these assets. These are not the only initiatives in the marketplace, but all of them have new architectural components, of which the network is an integral part.

New External Requirements and Pressures

The current unparalleled rate of reorganization within IT is having a profound impact not only on the underlying technology but also on the networking profession. CIOs love to make certain that their IT organizations are structured as they should be. This is especially true within an environment of economic downturns, emerging technology, and new processes. Network groups in particular get examined closely, because network operations provide fundamental support to all aspects of the business. In many instances, current networks actually hamper operations because of how they are organized and how they support the network.

Figure 2 shows a number of reasons for restructuring within IT departments. The four factors in the middle, outsourcing, globalization, mergers and acquisitions, and compliance, are critical external factors that are forcing radical changes in IT and network operations.

More and more companies have been outsourcing work during the last several decades. Yet one current trend is an increase in the overall number of outsourcing contracts that are up for renewal. The vast

![But restructuring efforts are subjecting the network to new external requirements and pressures](image)
The majority of outsourcing relationships are seven to ten years old. As companies decide whether to renew these contracts, many are not happy with the arrangements they have and actually would like to bring selective skills back home while continuing to outsource the rest. They are interested in bringing back networking skills in particular, especially in health care, because of security concerns. Security is an issue that is now intimately tied to the network. Companies want to be able to retain absolute control and they require an IT department that has the capability to master the necessary skill set.

Globalization is, obviously, a connectivity story. Employees, partners, and customers are spread around the globe and many of them require external access to business computer systems on a regular basis. IT staff are often located all over the world as well. How does a business make sure that it is constantly connected to all these people and entities, and capable of connecting to even more over time? IT staff, and the network team in particular, now must be able to support all that connectivity. It is essential that the networking team is not a bottleneck to increasing globalization and entrance into new markets.

Mergers and acquisitions impose a different set of requirements on IT departments. In the old IT world, it was often possible to have some sort of tie line connectivity into a newly acquired company that would enable a coarse level of information exchange. Until recently it was not necessary to rationalize all the programs across corporations. In today’s compliance environment, though, it is essential to make sure that everything is being monitored and tracked and done within the envelope of what is allowed. As a consequence, the capacity to accommodate mergers and acquisitions has become a key aspect of how well a network team engages in business activity. IT departments must effectively connect new networks and systems and enable remote monitoring.

The last external factor of note is compliance. In the current IT environment, some fairly simple questions need to be answered, including: Who has been on the network? How long have they been there? And what resources are they accessing? It is essential to have an audit trail of all user and IT operations and activities. It is also essential to control access to prevent unauthorized entry to IT resources. The answers to these questions have some technological components, but by and large this is an operational challenge. IT must make sure that it has the processes and tools in place to do access control.

In sum, outsourcing, globalization, mergers and acquisitions, and compliance are four of the biggest factors that are not only causing IT to restructure but also causing people to re-examine networking altogether.

### Changing Network Operations Skills

IT managers are favoring employees with a changing set of skills that enable managers to better align network operations with business demands. We can compare the traditional to the emerging skills:

**Traditional Network Operations Skills**

- Implementing routers and switches
- Designing WAN and LAN network typologies
- Securing remote access, setting up firewalls, and monitoring IPS/IDS
- Reporting on network availability metrics
- Troubleshooting network outages and equipment failures

**Emerging Network Operations Skills**

- Implementing mobile, UC, and TelePresence
- Designing complex networks for applications
- Tracking threats, protecting data, and providing network access control
- Reporting on application and user SLAs
- Troubleshooting content and performance issues

These changing tasks indicate a definite shift in the skill set that is required of the networking team. The new tasks are essentially analogs of the old ones. The original need to implement router switches has evolved into a need to implement a complex system that has mobility, unified communication (UC), and TelePresence all rolled into it.

Designing WAN and LAN network topologies has evolved into a need to implement much more complex application-oriented network software.

Data and system security has become a much larger concern with the vast increase in the range of user locations and applications. Security skills have been essential in the network domain for quite some time,
but they have been very technology focused around firewalls and reactive monitoring of intrusion protections. Now it is necessary to be much more proactive, due to compliance requirements focused on tracking and protecting data and controlling access.

Reporting has really moved from a handful of hardware-oriented metrics like availability and up-time to metrics around application and user SLAs. It may not matter so much if a network link goes down as long as all users and applications are still working. As long as it is still possible to track at the application layer, more valuable information can be obtained.

Troubleshooting, which is probably the lion’s share of what most engineering teams do, is evolving from hardware-oriented outages and equipment failures to content and performance issues. Often the database, the server, or a desktop component is actually the source of a problem. The networking team used to be able to do the root-cause analysis on issues like that and just troubleshoot the problem. If it was outside the network technology, they were expected to hand it off to the appropriate team to solve.

Widening Network Skills Gap

These changes in requisite skills are causing a widening gap between the skills that networking professionals have and those they need. This gap is detailed in Figure 3. The graph, despite the abundance of information on it, actually conveys a fairly simple truth, regardless of the size of an organization, the industry, or the geography. The bottom orange line shows the traditional capacity to learn new skills, which fits with the old rate of introduction of new technology. As some kinds of technology sunset, other new technologies come onboard. A certain amount of new knowledge gets taken in through the natural process of learning new skills. However, the blue line shows the accelerating rate of introduction of new technology. This is a significantly more exponential curve and indicates that new skills must be acquired at a much faster rate than before. This is an actual business requirement based on the factors driving the development of new IT initiatives, especially the four major external factors driving the need for restructuring networks.
Addressing These Challenges

IT Services Management

Nearly 60% of the participants in the Webcast on which this paper is based said that their organizations are struggling with gaps in technology, in staff skills, and even in staff numbers. In order to address the widening gap between the skills that networking professionals have and the ones they need, more effective IT departments are moving from a technology-oriented management approach to a services-oriented management approach, as shown in Figure 4. Historically, IT services management has been referred to as systems management. It is a series of tools and processes that allow organizations to have much more rigor in the way they go about managing their IT environment. Figure 4 shows a complex architectural stack, which essentially demonstrates IT services management from a control perspective. It delineates all the different services being managed from a command perspective across numerous different processes.

Process Frameworks

Process frameworks define management disciplines. IT service management is commonly broken into two domains, service delivery and service support, which interact with each other in a cyclic fashion. This is the approach most IT departments use to get ahead of the skills problem. These two domains typically include the following tasks:

Service Delivery
- Seek communication and project management skills.
- Create domain architectures that focus on blueprints of one to two years.
- Use tools and ITIL to standardize and automate service delivery.

Service Support
- Realign towers with a more process-based structure.
- Avoid “business alignment” at the expense of efficiency.
- Structure outsourcing with the ITIL framework for common language.

This approach is largely based on the Information Technology Infrastructure Library (ITIL), which is typically divided, at least from D3 on, into these two main domains.
service categories. Companies are selectively adopting ITIL to help with skills problems. ITIL is helping them adapt the way they are structured to provide them with the ability to align IT properly with the business. It allows for better outsourcing management because it enables everyone to work from a single vocabulary or glossary of all the different terms in the IT process. ITIL helps standardize tools. It also helps companies or divisions interface with other domains or architectures, such as the enterprise architecture staff versus the business process staff. It also aids in the development of some of the software skills needed in IT, which are centered on project management communication.

It may seem confusing to see a discussion about process frameworks and ITIL in what is primarily a network-oriented conversation. This is because the network has typically been isolated from this trend. The overarching process frameworks and IT service management tools have a really strong presence only in certain domains. Figure 5 shows this hierarchy. Strong management tools have been implemented primarily in the domains presented in green. Toward the bottom of this stack, shown in orange, are the network domains, which have suffered from the use of fairly weak domain-specific tools. While a lot of energy and commitment has been invested in changing the way people manage their networks, a gap has existed in the availability of good network management tools. That is why there are so few fluid connections between things like ITIL and associated data processes, or between change management, problem management, and infinite management and the network. The available tools have not been sufficiently mature to execute those processes. As indicated by responses to questions posed during the Webcast for this paper, the majority of participants believe that they are using acceptable network management tools. Yet about 94% say that there needs to be some kind of movement along the network management tools perspective.

There are several ways of looking at network management. It can be viewed from the top-down perspective of an analyst. Others focus laterally on network operations and the specifics of domain tool availability, including more specialized tools for issues such as Voice over IP (VoIP) and security. In either case, network management starts with a collection of tools that centralize command and control and provide workflows and policies that simplify network and security operations. This is shown diagrammatically in Figure 6.

Figure 5
Clearly, the network is part of a fabric of services that need to be managed. Because the network has typically been isolated from the process-frameworks approach, the first step is to bring it into the fold. Focus on those tools that allow centralized command and control. The days of CLI cowboys logging into routers and executing scripts no longer exist. Today’s network must be centralized and policy-oriented. It also has to have the proper workflow and enable many of the processes discussed previously. CIOs complain repeatedly that network teams are not policy focused; rather they focus too narrowly on technology or scripts. Thus they are not able to work across all the different domains required. They need to be able to work with the applications groups, the server groups, the storage groups, the security group, and other such divisions.

Network Management Tools

It is essential to select the right technologies in order to implement this centralized command and control model. While this has been difficult to do before now, network management tools are currently maturing with increased functionality. Considerable technological innovation and advancement has been made within this domain. Today’s improved network management tools include components that address modern needs for policies and services, automation, and security in an operationally cyclic manner.

Policies and Services

The capacity to deal adequately with corporate policies and services is at the forefront of any good network management tool. This cannot be just a bunch of binary options that an employee clicks into; rather, it must be a set of steps. Monitoring and report generation must be easy to accomplish and presented in clear and succinct formats to enable conversations with other elements of IT.

Automation

Automation is another important aspect of good network management tools. Whether the tool is specialized or designed as an overarching management tool, it must be able to automate many mundane but necessary tasks. This will free up quite a lot of IT staff time.

Security

Finally, good network management tools are designed with security in mind. Security simply cannot be bolted on as something that gets done separately.
Adequate capacity to address compliance and threat issues cannot be developed incrementally or by just doing the basic configuration of an ACL or something static. That circles back to the need for well-developed policies.

Those are the three attributes found in a good tool. Tools with these capacities probably did not exist even just three or four years ago.

**Closing the Skills Gap**

Investing in a good network management tool is critical also because it helps to close the skills gap discussed previously. Figure 7 shows how the capacity of network operators to learn new skills is augmented by automation so that IT can diminish the gap between what workers know and what they need to know. The orange line, which in Figure 3 was linear, begins to have more of the exponential curve that characterizes the blue one. The skills gap has not disappeared because business demands for new technologies continue to increase. But the implementation of a good network management tool has automated tasks, simplified policies, and focused operations on service delivery as opposed to the underlying technology. This has improved performance due to better operations, including:

- **Better SLAs**—Improves “soft” skills and the ability to articulate value to IT and business executives
- **Increased Efficiency**—Improves troubleshooting and aligns network operations with ITIL skills
- **Improved Client Satisfaction**—Improves visibility to streamline troubleshooting and focus on client issues
- **New Projects**—Allows networking team to focus on learning skills for new technologies

Recently, with a better network management tool, a large financial services company was able to have its entire network operations staff of about 100 people shift from 75% reactive, mostly as buyers, to about 50% reactive. That 25% compression allowed them to tackle new initiatives in the areas of security and virtualization. They became much more engaged in the technology initiatives that were on their 2008 docket. Ultimately, the better network management tool increased automation and simplicity and ultimately helped to close the skills gap. The staff was...
able to focus on soft skills, such as articulating the attributes and value of the network. The managed network is much more efficient because less time is spent troubleshooting. The network management tool makes it possible to reflect investments made in ITIL or process frameworks. It also enables improved client transactions. Many network engineers, especially level-three network resources, are no longer bogged down in archaic architectures. They can become much more involved in higher order issues, helping directly with customer spacing technology initiatives and not just configuring routers at the back end. And, as previously mentioned, it frees up time for new projects. New virtualization and security technologies and initiatives can be researched and deployed because the network team is available to do the work. These are all big benefits resulting directly in improved operations. Further, implementation of a good network management tool aligns the network with other parts of the data center higher up on the process maturity curve.

Getting Started

Implementation of a good network management tool must be accomplished in a rational way to be optimally effective. Prior to implementation, IT should identify key gaps and select the best platform.

Identify Key Gaps

Organizations frequently struggle with change management, problem management, and incident response issues from a network perspective. Most companies are very security oriented, but they have problems tracking, logging, and handling these issues in a consistent manner. So it is useful to begin the process of implementing a network management tool with a critical self-assessment that shows weaknesses and priorities for change.

ITIL is an effective self-assessment tool for identifying key gaps in network services management and skills. While it is not realistic or appropriate to implement the entire ITIL process framework within the network domain and enact all its best practices, it is beneficial to use ITIL selectively as a diagnostic test. It identifies and prioritizes problems and shows what areas network teams do particularly well or poorly. It can also help determine useful new roles within IT departments, such as Problem Manager.

Select the Right Platform

The second step in getting started with implementation involves selecting the right platform to optimize the process. It is essential to choose a centralized tool. It is surprising just how many network management tools do not provide a good centralized capability. It is also critical that the capability be simplified as well as centralized. It has to be one that is natively processed and policy oriented, so you can actually complete the security, automation, and other tasks that are required to help close the skills gap. Best-of-breed platforms are needed to help with network operations impacted by external drivers like security and compliance. The platform needs extensive APIs and the capability of integration with other management tools. Then, as network management matures, it will converge with other elements of infrastructure management.

Network management is not about picking a big, overarching management tool that does it all. This process is still very much about selecting best-of-breed products, the ones that are centralized and simplified and that walk you through the implementation. However, this cannot be done in isolation. That would only regenerate the problem of having network management isolated from other domains. So make sure the platform is very flexible. Make sure it is one that can be integrated as virtualization unfolds and that fits with corporate security demands. It absolutely has to be synced and boxed up with the network. Centralized tools need to have the various APIs, books, and ITIL that enable it to reach out and touch other domains. Be sure that the tool is tied together and enables many of those end-to-end processes.

Managing Today’s Networks

The central theme of this presentation is how we can employ centralized network management to increase efficiency, productivity, and security, and generally improve the network infrastructure by, in effect, simplifying complex processes.
Increased Network Infrastructure Complexity

Managing today’s network is not at all a simple task. Networks are becoming increasingly complex, beginning at the headquarters level and radiating from there. Some of the drivers that give rise to this increased complexity are globalization and changes in the economy, both upturns and downturns. Budgetary constraints and growing demands for Internet-based services impact network management as well, as technology advances and more people embrace the Internet. Further, companies must meet increasing regulatory requirements when they begin offering services, both to the public and to the people in their own organizations. Management and networking professionals are under a huge strain to keep up with this rapidly changing environment and the increasingly complex requirements it imposes on them.

Truly Distributed Networks

Globalization is driving a need for truly distributed networks. Distributed networks are those comprised of numerous IT locations. In addition to the headquarters location, a company may have affiliated sites all over the country or perhaps all over the world. Keeping an eye on the entire world can be very difficult, especially without some sort of cohesive network management tool, to hold the network together. Whether the company has five locations or forty does not really matter. At a certain point it is no longer practical to have administrators in each of those locations who can be available at a moment’s notice to address any issues that arise, whether connectivity problems, or a security incident, or something else. Having a central point of management where one or more administrators can react to a situation quickly reduces response times dramatically. More centralized networks make it possible to take care of problems right from headquarters. Administrators do not have to worry about what is happening on the other side of the planet.

Rapidly Changing Regulatory Requirements

Changing regulatory requirements play a huge role in driving the need for better network management tools. These demands imposed by regulatory requirements focus on a few key areas that get to the heart of why a centralized network management strategy makes more sense these days:

- **Continuity**—The global network must always be running, not just at the headquarters location but throughout the global infrastructure. Keeping services continually available to people at different sites in different countries is a challenging task.

- **Visibility**—Visibility is a very important aspect of regulatory requirements. Administrators and auditors need to be able to peer into the inner workings of the network and obtain information for a variety of different reasons. Having a network in which this information is available in a central location rather than several different locations will make IT departments much more agile. It will cut down on the amount of time necessary to take care of each task. With this time savings, staff can be assigned to other projects.

- **Transparency**—Transparency and visibility are closely interrelated. Transparency, however, focuses more on issues of concern to auditors and regulators, especially with respect to financial institutions, healthcare organizations, and entities of that nature. Transparency is absolutely critical. Auditors and regulators who may not be familiar with a system must nevertheless be able to get to the information they need quickly from all the devices within IT. Providing them with anything that they want to see takes time, energy, and effort. Often employees must be pulled off other projects to cull this information from myriad locations. With a more central network management strategy, this process becomes very simple. Point configurations with disparate devices do not lend themselves to transparency because of their complexity.

- **Adaptability**—Adaptability is another key consideration. Organizations need to have global infrastructures that are changeable and agile. Organizations must be able to think quickly and to address security concerns proactively rather than reactively.

Ensuring Security and Resilient Connectivity

Security and resilient connectivity are two important concerns that go hand in hand. A secure network is less likely to be negatively impacted in a way that reduces organizational connectivity, including resilient connectivity at the ISP hardware level. Firewalls and other intrusion-prevention devices must enable the network to be resilient and always available. If something disastrous happens, it is essential at least to have basic data available again very quickly. Managers, employees, and customers are becoming...
increasingly demanding and diminishingly fault tolerant.

**Turning Data into Intelligence**

It is critical to be able to take data from all the different devices in the network and turn it into useful intelligence. Yet it is a colossal waste of time to take bits of data in tiny snippets and chunks and spend hours correlating them into a cohesive picture. It is important to have a tool that can do that by itself, culling and assembling data from all the different areas of the network. This improves agility and provides the capacity to improve the network through improved knowledge.

**The Maze of Network Management Options**

A maze of network management options is available today. Point configurations, shown in Figure 8, are common but do not lend themselves to a great deal of agility. This type of solution cobbles together devices made by several different vendors and consequently does not really have a central focus of control. The devices are not on a common platform. They are fragmented, so the network is fragmented. This creates silos of knowledge, which can be a big problem. With silos of knowledge, certain people are experts in particular network devices. But if something happens to an expert, especially with turnover in an organization, it may be necessary to spend a lot of time reinventing the wheel. This exacerbates the skills gap rather than reduces it and separates that linear curve even further from the exponential one. This is not very efficient. Multiple administrators need to pass the torch of knowledge and information. This is inherently impossible with disparate devices and no cohesive way to manage them all.

**The StoneGate Platform**

A better way to address and solve these problems is a centralized network management option like the StoneGate Management Platform, illustrated in Figure 9. The StoneGate Management Platform directly addresses many of the points discussed here because it is inherently a centralized management solution. From management all the way down to the firewalls, the IPS, and the secured remote connectivity, all the devices reside on a common platform. All can communicate with one another. They all log their data to a location that allows administrators to pull that information quickly. This extremely detailed
Information enables managers to get what they need very quickly. The workflow and layout of the design were built logically. Data does not reside in odd, idiosyncratic locations because there is an underlying logic that holds the whole system together. All the devices logging into the same location speak a common language and communicate with one another while allowing for multiple administrators. That improves efficiency. It cuts down on time wasted, which saves money. Passing the torch is possible even with multiple network administrators around the world. They are all using a common platform in a central location. Communication between these administrators is possible, so that one does not interfere with what the other is doing and vice versa.

Centralized management encompasses many different components. True centralized management with the StoneGate Platform includes:

- One scalable management platform for both physical and virtual environments
- Interoperability and communication among managed devices
- Operating system-independent GUI client
- Robust, flexible, and customizable management tools
- Real-time monitoring of security devices, security events, and device status
- Role-based administration
- Truly multi-user
- Automated system tasks, such as backups, upgrades, and updates
- Alert escalation system
- Log-data and security-incident management tools
- Integrated reporting, compliance, and auditing tools
- Highly available management

It is especially important to have a system with resilient connectivity and a centralized management system that is highly available. If your firewalls, IPS, SWAP, and other parts of the system are highly available, then the management system should be highly available as well. If your management system in one location is damaged, then all that data is available on another system, which can come up with a moment’s notice to manage the remaining devices.

Figure 9
Communication between modern managed devices is absolutely critical. They must be able to talk to one another. The IPS and firewalls need to communicate with one another. Because the StoneGate solution all resides on a common platform, this communication is inherently possible. IT needs a management system that is not stack, that is dynamic and very customizable. Not every administrator is the same and wants the same things as every other. Each wants to see information of interest to him or her rather than fishing for it at every log-in. Administrators need the information they want available to them immediately. So it is important to have a product that is customizable.

Real-time monitoring of security concerns is very directly proactive. If there is no real visibility into a device and something unforeseen happens to it, IT is forced into a reactive mode immediately. But with real-time monitoring, there are no surprises. The status and all other aspects of a device are visible, such as the expand speed temperature of the central processing unit or the capacity of the hard drive. IT is alerted before issues become problems and can handle the situation proactively.

Role-based administration is another aspect that is absolutely critical. Different administrators at different levels of the organization require different levels of access. For example, an auditor who does not have any business manipulating objects within the system must be able to retrieve necessary data without the possibility of changing it. When the auditor’s work is finished, his access privileges can be disabled. Clearly, role-based administration with predefined roles is very important.

The capacity to accommodate multiple types of users is also very important. Managers, networking staff, auditors, and others will all need access. It is completely impractical to have a system that can be accessed by only one type of user.

An alert escalation system is vital. This system ensures that security incidents are not overlooked. Whether the escalation system is built into the system or IT configures it, a backup process must be in place. When one administrator does not respond, the system must automatically escalate so that another does respond and takes care of the incident before it becomes a real problem.

These capacities can be found in most centralized management systems. But they are all built right into the StoneGate Management System, which makes it a particularly good choice.

**Recommendations**

**Determine the Right Place to Start**

The first task is to assess which network management system is most suitable for the company. A good way to begin is by conducting an internal needs analysis. What are the most pressing issues facing your infrastructure? Secured remote connectivity? Resilient, always-on availability of Internet services? What are the issues for the IT department, other managers, and customers? Is it possible to recover quickly when problems occur? If one or two or three Internet service providers go down, what can be done? What is the best way to address the issue without piling on tons and tons of hardware? Essentially, what are the pain points? These are the questions that need to be asked.

**Choose the Best Partner**

After the specific needs of the company have been determined, potential management systems can be evaluated for goodness of fit. The following aspects are of particular concern:

- Do their solutions provide visibility across networks, both physical and virtual?
- Can security and connectivity issues be addressed quickly? How agile is it—really?
- What impact does their solution have on network performance?
- How easy are their solutions to use and manage?
- What is the total cost of ownership (TCO)?
- Is the solution scalable to future needs?

Once these questions are answered, the next thing to do is to choose a partner that can really help meet all the company’s needs. It is important to select a partner that knows this technology inside and out, for whom this is their bread and butter. They also need to be flexible. They need to be able to grow along with your company and continue to address concerns that may be specific to your organization, not just the lowest-common-denominator issues of their entire customer base. If the company goes virtual but still has physical firewalls, will it be possible to have both without adding another dashboard or some other program for management? It is important to have a
partner that enables IT to be agile and quick and to address connectivity and security issues. It is also desirable to have a partner who will be available to assist in rounding out the entire IT security framework.

Establish the Most Important Metrics
Determining whether and in what ways the implementation of a network management solution has enhanced performance requires detailing specific performance-evaluation metrics. If at the exterior of the network, or even at its core, capacity grows and the sizes of the Internet files and internal files grow, will the solution scale adequately? Is it easy to manage and will increasing capacity make it more complex to manage? Is the bottom-line total cost of ownership reasonable? Once the right questions have been determined, then it will be necessary to measure, measure, measure to find the answers. After that it will be possible to decide which partner company and network management solution will best help the company execute its IT strategy.

While other options are available, many customers are very happy with the centralized network management approach found in the StoneGate Platform. One customer said, “The minute we turned on Stonesoft’s solution, it was like turning on a light switch. Immediately we had analysis and reports that provided clear details of who and what was trying to access our network, which enabled us to diffuse potential threats ahead of time.” Another said, “With StoneGate’s unified firewall-VPN-IPS solution, we have a proactive threat-management solution combined with the advanced auditing tools we need that gives us a distinct competitive advantage.” And a third said, “StoneGate provided the most immediate ROI and the lowest TCO, all while addressing our needs for resilient connectivity and improving our network performance from a unified management system perspective.” Clearly the StoneGate Platform is an option worth considering.
Question: What is the most important feature of a good management tool?

Answer: Traditionally companies have focused on the scalability of the platform or how it interacts with all the different systems and whether it is heterogeneous. More important, however, is whether or not it has a good policy interface. In just the last couple of years there was a huge shift away from teleneting, specific underlying scripting sessions, and things like that. Now there is a much more policy-oriented way of managing the network. It is abstracted, in a sense, to be able to handle the more complex tasks that are required at the network level today. Some vendors have tools that include policy management. But it is hard to get anything done with these. You end up having to supplement all sorts of other tasks. This becomes a complete mess from a centralized perspective. So make sure that the management tool has a really clean policy interface that makes it possible to fix things that may not work well. This also allows you to do reporting and things like that as the network becomes a more critical component within IT. It is good to be able to articulate that back to the business when they are wondering what IT has done for them lately.

Question: How important is it to have a single network management tool?

Answer: It would be a mistake to just have one single network management tool. In fact, that is true of all IT domains. You will find that some tools excel at automation, some at reporting, and some at security. If it is possible to focus on the things discussed during the presentation, such as adaptability and the policy interface, then the tool will provide a great deal of increased efficiency. That is much better than going with a single tool that gives you sort of a red, green, and yellow view of the network simultaneously. That may be good, but it is not actionable. It is not possible to execute some of the necessary tasks from there. Also, such a tool is not adequate to deal with some of the important emerging skills. So it is a mistake to think you have to have only one tool. You should instead try to consolidate a certain number of tools that can help you with all the different processes that need to get done.

Question: How important is it to have separate security versus centralized network management tools?

Answer: Security capabilities and security skill sets have migrated toward the networking team in recent years. It is something that they have taken over because it is operationally efficient. Yet it is still important to maintain the best of every tool set. It is still important to have a tool that can help with the workflow that is specific to a security environment. As mentioned before, it is about being able to answer a series of questions such as: Who is on the network? How long have they been there? What systems are they accessing? But it is essential to be able to do that in an established process way. It is not good to obtain that information by pulling up data from a bunch of separate platforms and having to deduce a story from it. So the key is to absolutely use that central tool. The problem with the big, overarching network management tools is that they simply do not provide the depth necessary. So if you are suffering that skills gap highlighted earlier, then you still need to supplement the management tool with a security tool. However, do not go after every security widget. Every security widget has its own separate security management tool so that you end up with 10 security tools to go about fixing that one problem. It is important to centralize and simplify as much of that as possible. But, of course, you also do not want to go to the other extreme in which you get some overarching network management tool that does not go deep enough. So there is definitely a sweet spot in this domain. Stone-soft’s approach is really one of the best approaches to handling security.
About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our events give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via specialized e-Newsletters, video TechTalks, podcasts, blogs, and wikis. Our Webcasts allow IT pros to ask questions of technical experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events, the expert interaction of Webcasts, the laser-targeting of e-Newsletters, and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals.