

Introducing

E-zones

Preface

Innovation and Collaboration Drive Success

Innovation lies at the heart of Motorola's success. To fuel innovation and conduct business, thousands of people both inside and outside our company depend daily on the availability of information and the ability to share it. When we were a vertically integrated player in the communications market, the walls we built to protect that vital information served us well. They helped us to "hold our cards closely."

Today, however, those same walls are preventing the level of partner collaboration we need to stay ahead in a much broader market. It is an important issue. At stake is our ability to collaborate, innovate and compete as a leader in our industry. The opportunity is great, the solutions are available, and within our organization, we can rise to the challenge and realize the rewards of an open communication and innovation environment.

Where Do Our Current Systems Fall Short?

Successful companies of today leverage information heavily (e.g. eBay and Google). They enable information sharing that in a peer to peer manner allows for unstructured collaboration and the ability to create and capitalize on new opportunities.

The vision of seamless mobility encompasses individual access to information from anywhere, at anytime, on any device. This is an empowering vision; however, our current networks were never designed to provide such access while protecting critical digital assets of our company (intellectual property, financial data, personally identifiable private information of customers and employees). We must evolve our systems and practices to support and execute on the Seamless Mobility vision. Innovation is part of Motorola's heritage and competitive edge. E-zones will enable us to innovate faster and more easily than our current environment allows.

Balancing Information Protection and Information Access

Some of our information must be protected to comply with laws, regulations and company policies that support business objectives. However, much of it is not subject to strict controls. If Motorola is to encourage collaboration, communication and rapid innovation, we must encourage as much sharing of as much information as possible with limited friction. A new information sharing model for Motorola must enable collaborative connectivity while increasing information protection and network resiliency. This approach must give internal business units and other functional groups both responsibility and capability to control their information destiny.

The Goal: Realize the Opportunities of "Open Innovation through Collaboration"

We must change our approach to one that enables access while managing risks. We must transition from a mindset and tool set which is closed-by-default to one that provides flexible access policies which match the requirements of the data. We must retool our policies, processes and technology, then train and support our people to put those changes into practice.

This paper focuses on the changes to the IT environment needed to align our systems, the people that use them and the assets they contain to create an infrastructure which can capitalize on the opportunities of "open innovation through collaboration."

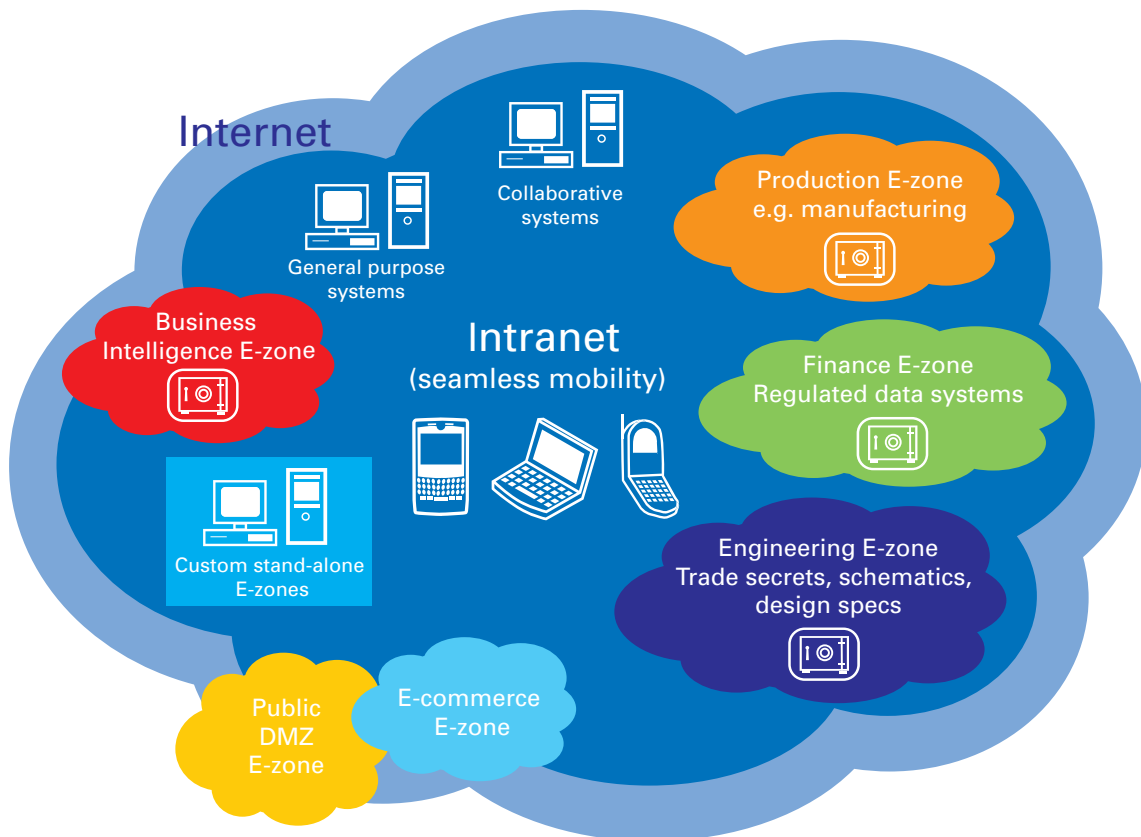


CONTENTS:

- 4 Introduction
- 8 Key Benefits of E-zones
- 11 User Access and Data Protection
- 13 Moving Forward
- 15 Conclusion

FOR MORE INFORMATION
CONTACT:
Scott Shepard +1-847.576.8894
Bill Boni +1-847-576-8884

The E-zones architecture is a proposed new approach to information access and data protection. E-zones facilitate sharing of information with Motorola's mobile employees, business partners and customers, while improving the protection of critical business data.



Introduction

The proposed E-zones architecture supports seamless internal and external network connectivity, resilient operations and highly collaborative business initiatives.

E-zones are the organizing principles for a proposed new approach to network access and network protection at Motorola. The goal is flexible, adaptive employee and partner connectivity for improved collaboration and continual business process innovation. The E-zones architecture will help create a Motorola IT infrastructure that delivers on the promise of seamless mobility in a wide range of business and consumer markets.

Note to readers: This paper serves as an executive introduction and overview for the E-zones model. Please see the companion paper, "E-zones Technical Architecture" for design and deployment details.

E-zones reduce security hassles.

How will E-zones change the security user experience at Motorola?

Current Environment: "No Way"

E-zones: "No Hassle"

Ask Motorola managers how they feel about internal security requirements today and—at best—you'll hear begrudging acceptance of security as a necessary evil. The reason is simple. In the current monolithic security infrastructure, restrictive policies must be applied enterprise-wide to protect all of Motorola's daily data-flow when only a small portion of data requires protection. E-zones is a new security architecture that will change the security user experience from "no way" to "no hassle."



Open Innovation in a Time of Change and Uncertainty

Since releasing DynaTAC as the first commercial handheld cellular phone in 1983, Motorola has created an impressive string of innovative communications products at an ever-accelerating time-to-market pace. Many competitive contests were won during this busy period as Motorola invented and reinvented business processes to support demanding design, manufacturing and delivery requirements.

Today's challenges, however, are beginning make those of the last two decades look tame. The technology landscape is highly dynamic and the global competitive pressures that Motorola now faces are extreme. A central aspect of the current business climate is an accelerating rate of change. Leading strategy mavens John Hegel and John Seely Brown put it this way:

“As change accelerates, something interesting happens – and it can be very unsettling to leaders of large, established institutions. All of a sudden, what we know – those “stocks” of knowledge – becomes less valuable.... Now, the game becomes using our knowledge as a way to connect more rapidly and effectively with others to create new knowledge. Stocks of knowledge become progressively less valuable while flows of knowledge – the relationships that can help to generate new knowledge – become more and more valuable.”

Brown and Hegel believe that market excellence is best achieved by establishing diverse bi-directional knowledge flows. These knowledge flows comprise partners, suppliers and an army of specialists all interacting creatively within a loosely coupled collaborative framework that enables “open innovation.” They cite stunning examples from Asia of complex knowledge flows between an ever-shifting mix of participants. These knowledge flows enabled fast-paced and high

quality design and manufacturing successes in markets ranging from textiles to electronics. When organized and supported with Internet-style computing, mobile devices and Web services, collaborative knowledge flows can become dynamic learning ecologies. These flows can drive continual innovation and yield a sustained competitive edge. They enable and require large companies to rely less on static stores of existing intellectual property and internal creativity, while relying more on network-based information flows between large numbers of internal and external participants. Unrestricted knowledge flows also facilitate continual process improvement, enabling quality methods that require high levels of feedback through a virtual community of stakeholders in different locations.

.....
An open and agile enterprise network architecture is essential for companies seeking to reap the benefits of unrestricted knowledge flow.
.....

The Network Roadblock

In large enterprises, network access and security controls have often become roadblocks for organizational and operational change. There are several reasons for this. Historically, network architectures have been oriented towards the single isolated enterprise with critical resources and processes behind the corporate firewall. The traditional networking model uses an enclosing perimeter defense to create a corporate “data fortress.” Reaching out to customers and external partners has been the exception, not the rule. Links to partners are made with expensive, tightly coupled connections (e.g., custom extranets), as opposed to the loosely coupled, low cost, standards-based internet connections (e.g., XML, service-oriented architectures, Web services).

Another cause for the “network roadblock” is the recent explosion of network-based viruses, worms, Trojan horses and hacker exploits. To respond to these threats, enterprise network access policies and security controls focus more on traffic blocking



and user restraints, and focus less on innovation initiatives and business process enablement.

Knowledge flows can be particularly productive within service-based interest communities where a unique mix of competencies and specialties convene (e.g. collaboration with specialized design

and manufacturing partners around the world; strategic process outsourcing; extended supply chain, etc.). Unfortunately, enterprise networks have become an obstacle for executives and business unit managers who want to use desktop, data center and handheld resources to set up such knowledge flows.

Innovation and Knowledge Flows at Toyota

John Seely Brown speaks of his plant floor experiences:

“Toyota has found a way to tap the creativity of thousands of their suppliers and their own employees in terms of creating new ideas and new innovations through the notion of **productive friction**.”

“They build long term relationships with their suppliers and they expect the suppliers to actually push back on them. They say [to suppliers] here’s what we kind of want, or here’s what we exactly want, and the suppliers - both first, second and third tier suppliers - are allowed to come back and say, ‘Well you know, if you thought about doing it this way, we could actually do it a hell of a lot cheaper.’

So Toyota can, through productive friction, find new ways to build parts and change the design of the automobile or sub-assemblies. It’s very interesting to see the ongoing network of conversations and the productive friction that is happening there.”

- John Seely Brown, address to Super Nova Conference, San Francisco, June 2005.

The Perimeter Firewall is Failing

For over ten years, the main tool for protecting corporate IT resources has been the **perimeter firewall** (See Figure 1.) The perimeter firewall is a gatekeeper that enables appropriate network connections to the outside world. It is also responsible for blocking any unauthorized traffic into or out of the enterprise. In essence, the corporate perimeter firewall is both connector and protector.

As **protector**, the perimeter firewall is supposed to insulate enterprise users and digital assets from external threats. But the average enterprise has hundreds, and in some cases thousands, of holes in its firewall to allow VPN’s, SSL tunnels, Web-enabled applications, remote connections by mobile users and other external links. As a result of these perimeter breaches (and increasing internal threats as well), enterprises are now more susceptible than ever to viruses, worms, Trojan horses and other forms of malicious attack. In today’s complex IT environment, corporate perimeter firewalls provide only a crude defense against attacks. This is due largely to the fact that

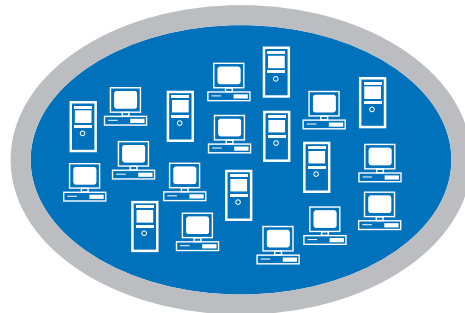


Fig. 1 The perimeter firewall bundles all internal users, applications and data into the same protection area.



they bundle all internal users, applications and data into the same monolithic protection area. As a result some assets have too much protection and other assets have too little protection.

As **connector**, the corporate perimeter firewall is not the best approach for creating flexible connections to external partners, suppliers and mobile workers. The difficulties of protecting assets with a single, monolithic perimeter firewall mean that requests for new network connections to remote workers and external partners take too long.

.....
The corporate perimeter firewall defense is no longer optimal or adequate in terms of connection or protection.
.....

E-zones Arrive

Forward-thinking technologists and IT executives agree that perimeter firewall-based networks must be rethought and redesigned. Fortunately, alternative approaches have emerged. Building on proven best practices and early adoption successes at companies such as Goldman Sachs, this paper proposes a new networking model for Motorola. This model places the emphasis on collaborative connectivity while at the same time increasing capabilities in the area of data protection and resiliency.

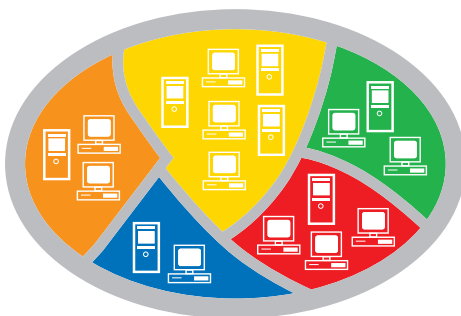


Fig. 2 E-zones provide areas of connection for users, applications and systems that share similar needs for connectivity and protection.

The primary building block of the proposed network architecture is the **enablement zone** (E-zone), a logical collection of users, software applications and systems that have a similar need for connectivity and protection. A business unit, department or functional unit can support any number of E-zones, and there can be any number of systems per zone. E-zones can be short-term (project-based) or permanent.

An E-zone has these characteristics:

- Ease-of-use for users, managers and administrators
- A well-defined information protection posture balancing protection and connection
- A set of “roles” defining typical user activities and access rights
- Organized and defined using any business, operational, financial or risk management criteria
- Can be given a specific level of network performance and quality of service

The “protection” aspects of E-zones facilitates improved compliance to Sarbanes-Oxley (SOX) guidelines, General Financial Controls, privacy laws and related regulations and audit requirements. The policies and procedures associated with each E-zone enforce **compliance by design**. Compared to the current security perimeter approach, E-zones are a greatly improved method for financial and confidential information protection and data integrity, allowing stricter control over the storage and disclosure of sensitive and valuable digital assets.

The “connection” aspects of E-zones include easier network access and faster time to network connectivity. These advantages can lead to increased business agility and better support for cross-functional initiatives both inside and across the firm’s boundaries. Along with increased productivity for network users comes potentially significant improvements for the ROI of network-based investments. It is expected that E-zones will significantly lower the operational costs associated



with network administration and compliance over time. Because E-zones are a true enabler of agile processes, there are also important implications for reducing the lost opportunity costs associated with weak network infrastructure.

KEY BENEFITS OF E-ZONES

Balancing Protection and Connection

The goal of an enterprise network is to provide high levels of connectivity for legitimate users and protection from threats and dishonest users. Practically speaking, however, it is virtually impossible to have both maximum protection and maximum external connectivity at the same time. At one extreme, the most protected information assets can be isolated in a data center with no external connections. At the other extreme, information assets can be accessed by anyone on the public Internet, reducing protection somewhat

but not completely. For most E-zones, the right balance of protection and connection will be somewhere between these extremes. Figure 3a shows how the current perimeter firewall defense achieves neither protection nor connection very well. In contrast, E-zones allow Motorola business managers to choose appropriate levels of protection and connection for each functional group of users and IT resources. For example, in Figure 3b, a finance manager chooses high levels of protection for SOX Level 1 systems and limited connectivity to the outside world. In Figure 3c, a supply chain logistics manager chooses more connectivity and less protection to facilitate easy collaboration with external partners and suppliers.

The layered E-zone model also lends itself to advanced n-tier application models that are the basis for extended Enterprise Resource Planning (ERP), extended supply chains, Customer

E-zones enable agility

Time to provision secure connectivity with vendors, partners and customers:

Current Environment: 30 to 180 days

E-zones: 3 to 10 days

Motorola's ability to innovate and cost-effectively create value for its customers is inextricably tied to our ability to securely extend the electronic working environment to include vendors, partners and customers. E-zones will deliver an order-of-magnitude improvement in provisioning time for secure connectivity. As a result, alternative means of exchanging information will be replaced by extensible infrastructure that enables increased agility.



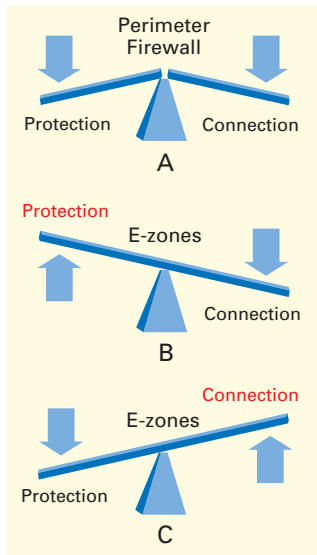


Fig. 3 Unlike perimeter firewall-based architectures, E-zones provide the flexibility to balance varying needs for user connectivity and protection of data.

Relationship Management (CRM) applications and high performance ecommerce services. In this case, a Web server in a public E-zone could access an application server in a mid-tier zone, which in turn could access a highly secure database server that cannot be reached directly by users who are not in its zone.

Heightened Protection for “Data of Concern”

One of the most important qualities of E-zones is the ability to give “Data of Concern” a higher level of protection than less sensitive data. Defined as information whose use or access is limited by laws, regulations or company policy, Data of Concern comprises an estimated 5 - 10% of all Motorola data. With E-zones, Data of Concern will reside in locations protected by methods such as intrusion detection and strong authentication (e.g. tokens, smartcards, or biometrics) The remaining 90 – 95% less valuable data will reside in more accessible zones.

Some examples of potential Data of Concern, include:

- Marketing introduction plans
- Product designs
- Source code
- Pre-patent inventions and research
- Level 1 SOX data
- Merger and acquisition plans
- Pre-release performance information

- Personally identifying information (PII)
- Motorola customer credit card numbers

E-zones and Policy

E-zones move the enterprise away from a “one-size-fits-all” model of network access and protection. To accomplish this move, new policies and procedures are required. In the current centrally managed model, business unit managers and department heads are subject to a patchwork of fragmented, overlapping and sometimes contradictory policies, including hundreds of pages of company security policies, procedures and guidelines.

E-zones provide a platform for a complete reorganization and streamlining of network and security policy. This occurs because: a) E-zones greatly simplify policy by organizing it into a consistent hierarchical framework; b) E-zones put the responsibility for compliance with policies in the hands of business and functional managers.

The streamlining and simplification of network related policies is embodied in a new Motorola **Information Protection Framework**. This framework consolidates a majority of existing policies and organizes them in a top-down

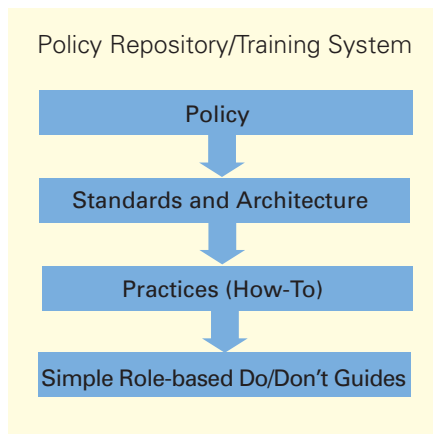


Fig. 4 The Motorola Information Protection Framework consolidates a majority of existing policies and organizes them in a top-down structure that includes easy-to-follow best practices and user do/don't guides.



E-zones: What's in a Name?

In a general sense, the "E" in E-zones stands for "enablement, but it can also have different significance for different stakeholders.

End-users: "E" stands for **easy**.

Finance: "E" stands for **enforcement** of laws and regulations.

Supply Chain: "E" stands for **expedite**.

Business Unit Managers: "E" stands for **efficiency**.

The risk management committee: "E" stands for **emancipation** from hidden and unexamined risk!

structure that includes easy-to-follow best practices and user do/don't guides. This allows users to be protected with the policies that are most relevant to their day-to-day roles without overwhelming them with the volume of policies required in the current ubiquitous protection environment.

The framework is intended to be a practical working tool to apply policies that ensure that people, processes, and technologies work together with the right balance of protection and connection.

Each element of the Information Protection Framework maps back to relevant standards, regulations and governance decisions. By operating in the Information Protection Framework as they apply network policies, managers have assurance that they are not out of compliance or in violation of strategic business and risk parameters.

End-User Roles

In the current system, considerable expense and delays are incurred by the ongoing chore of administering network user accounts and privileges. The task of managing accounts is made particularly arduous because it must be done repeatedly on a case-by-case basis. E-zones depart from this cumbersome model by applying access permissions and network rights based on standardized user profiles or "roles" that conform to policies within the Information Protection Framework.

User roles can accommodate any user behavior: e.g., a temp accessing low risk marketing boilerplate and templates, or a finance manager accessing sensitive earnings data. An engineering user role may give access to design data and Computer Aided Engineering (CAE) systems. A logistics role gives access to supply chain and distribution systems; and so on. Some factors that contribute to role definition include:

- Business value of target data
- Location of user and target application
- Usage patterns (24x7 vs business hours vs occasional)
- Data modification needs (read only vs batch vs read/write)
- Job title or organizational function, etc.

Once roles have been defined and those roles have been given rights to certain data and IT resources, they can be applied rapidly and easily to any number of users, greatly reducing complexity and redundancy in network administration.

E-zones for Risk Management Empowerment

In the current centrally managed firewall model, business and functional managers have no choice but to accept the risks of using the network. They have little or no control over risk management decisions that impact information assets. For example, if a valuable design schematic is stolen via the network, the manager who owns that data is unable to make protection adjustments to



prevent it from happening again. In the current system, the IT and security staff are only nominally in control of risk. As a result, risk management often remains unaddressed from a business case perspective.

An E-zone solution gives managers the ability to assess the risk associated with their group's data and then take actions to protect any data of concern. Managers can make their own decisions about whether to accept the risk or what level of investment they are willing to make to protect that information. Consequently, E-zones enable risk management self-determinism for the managers and process owners who are best qualified to judge what assets have a high risk associated with them.

In the context of the current deteriorating perimeter defense, data theft, data loss and data corruption are ever present threats. These threats create a climate of uncertainty and reactive, after-the-fact responses. E-zones enable risks to be better understood and managed through the balanced combination of both preventative measures and response. E-zones are a powerful tool for risk compartmentalization. Compartmented risk effectively reduces enterprise and business unit risk profiles, allowing targeted protection of valuable Data of Concern.

To coordinate risk management efforts at the strategic level, a proposed **Information Risk Management Board** will be established with representatives from business units, finance, HR,

E-zones Provide Protection

Protection of personally identifiable information for employees and customers:

Current Environment: High risk of unauthorized access to employee and customer data

E-zones: Defense-in-depth approach improves security of sensitive personal information

In 2006, several highly publicized incidents involving unauthorized disclosure or theft of confidential data underscored the importance of protecting personally identifiable information. In addition to severe financial and legal implications, unauthorized disclosure or theft of data can result in irreparable brand damage. E-zones brings a defense-in-depth approach to protecting confidential records and other Data of Concern, combining compartmentalization with Identity and Access Management (IAM) and Information Rights Management (IRM).



IT, legal, sales, supply chain and other key groups. The risk board will serve as a clearinghouse for high level decisions concerning data and information protection issues.

USER ACCESS AND DATA PROTECTION

Managing User Access:

E-zones and Identity Management

Enterprise networks and user populations continue to grow increasingly dynamic and varied in their needs. As a result, streamlining the process for identifying and classifying users and giving them rights to network-based assets has become a priority. The typical corporate user needs access to a range of applications, often in more than one functional area. To streamline access management, users can be given role-based network accounts that are standardized across multiple E-zones, applications and systems across the enterprise. The result is an Identity and Access Management (IAM) function that helps the organization realize several significant advantages:

- **Lower Costs:** Reduces the administrative costs of setting-up and eliminating user accounts.
- **Minimize Frustration:** Reduces the effort and confusion associated with using multiple passwords, security tokens and accounts.
- **Reduce Risk:** Reduces fraud and misuse of IT assets that result from weaknesses in current fragmented authentication and access systems

IAM maintains a single identity and profile for each user. This identity can be used to access IT resources in multiple zones and ultimately in multiple enterprises. IAM systems could eventually achieve the coveted "single sign-on" capability, enabling users to access any systems and applications to which their identity has rights. Such a capability would allow the fluid use of many different systems without interruption. Without identity management systems, some

Expert Definition of Zoned Architectures:

The Burton Group, a leading enterprise infrastructure consultancy, defines the zones model as: "An aggregation of network resources that have similar protection requirements and compatible content....it is critical that the organization divide the network into zones with an understanding of the risk posed by necessary communications to the [zone's] resources or systems."

"...the notion of the hard shell [corporate] perimeter is disappearing," says Phil Schacter, analyst with Burton Group. "The perimeter is being distributed to many different places in the infrastructure, which creates the need to attach to private networks."

"Security and Risk Management Strategies - Perimeters and Zones"
Eric Maiwald, The Burton Group
April 2006

experts predict that large enterprises will reach a crisis point in password and access management in the next few years.

Because E-zones integrate people, processes, policy and technology, they are fully compatible with a wide range of advanced IAM, automated access management tools, XML-based directory services and automated provisioning systems.

Managing Data Accessibility:

E-zones and Information Rights Management

Identity systems manage unified information about user profiles and access rights. Information Rights



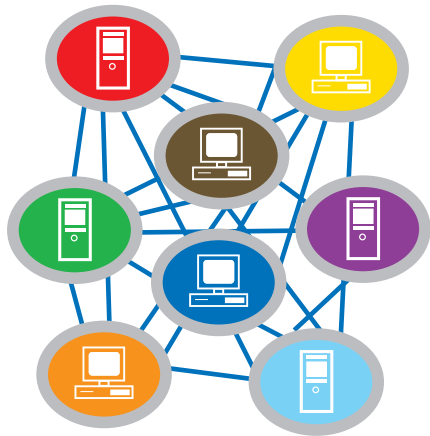


Fig. 5 Future models will replace perimeter approach with methods that directly protect end stations and applications, enabling fluid connectivity between organizations and enterprises.

Management (IRM) compliments IAM by creating “profiles” and access rights for data. IRM controls the distribution, copying and printing of individual pieces of data, including spreadsheets, databases, documents and various digital media objects (video files, audio files, images, etc.). IRM can be used to control and monitor access to virtually any digital asset. Using advanced encryption methods, IRM places a protective “wrapper” around data, ensuring that only those with the proper identity or credentials can access that data. IRM requires users to “log into” data in much the same way users log in to systems on a regular basis today. IRM is particularly well-suited to support Data of

Concern protection in an E-zones architecture, because IRM provides a method for files to carry their protection beyond the zone. When a file leaves a protected E-zone, it can be encrypted with IRM and granted specific permissions that map to users’ identity and access rights. IRM prevents unauthorized access to ensure accountability and high levels of compliance and data privacy. It is important to note that IRM is not widely available yet and there is much work to do to integrate IRM with existing data and applications. The evolution to ubiquitous IRM will be gradual, but this work has already started and will likely reach critical mass over the next few years.

MOVING FORWARD

E-zones for an Enterprise Without Boundaries

The implementation of E-zones, IRM and IAM will set the stage for highly advanced forms of network access and protection. Many of these approaches are already being tested using the principle that security should be placed as close to the data as possible. Increasingly, planners are recognizing that placing strong encryption, authentication, intrusion protection and rights management at the application level on each individual end system is a highly effective approach. (See Fig. 5) This is almost a complete reversal of the current perimeter firewall model. When end-systems, applications and data are

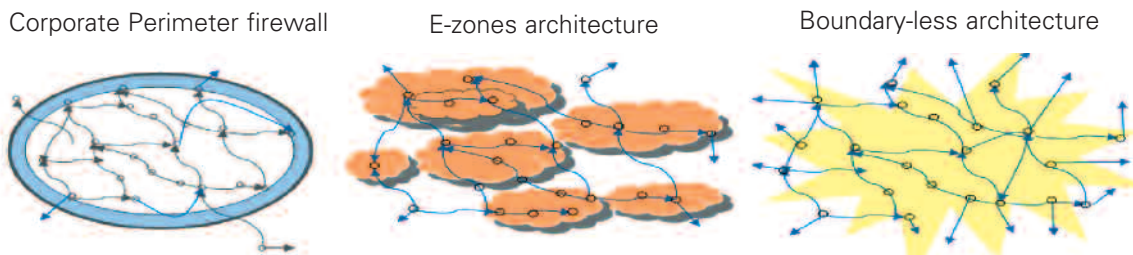


Fig. 6 E-zones represent a key step in the evolution from cumbersome corporate firewall based “perimeter” systems, to the highly agile boundary-less architecture of the future.



truly secure, there is much less need for complex, expensive monolithic network security (firewalls, intrusion protection, vulnerability analyzers, etc.). The following analogy describes the evolution from a single monolithic perimeter firewall to E-zones, and finally to secure end systems with an open network:

In the Middle Ages and earlier, towns were often protected by sturdy walls that ran around their perimeter. Houses did not have very good built-in protection, so the town perimeter wall was the main line of defense. But over time, as thieves and criminals found ways around outer defenses, smaller defense perimeters were erected around more local neighborhood areas, which developed their own internal guard forces, etc. Today of

course, houses have their own robust locks and alarm systems, so town walls and neighborhood level security are not as important.

So, from the traditional corporate perimeter firewall, we are evolving to secure E-zones as a more granular form of protection and a more granular control of network access. Ultimately, as end systems and data get their own local protections (strong authentication, access control, intrusion detection, personal firewalls), the network can open up greatly as perimeter and zone defenses are lowered.

The combination of E-zones, IAM and IRM create a favorable environment for moving toward a boundary-less architecture. (See Fig. 6) This

E-zones empower collaboration

Collaboration between employees, partners, customers and vendors

Current Environment: Popular collaboration tools and technologies are too risky to support.

E-zones: Emerging collaboration tools speed exchange of ideas without adding unacceptable risk

Just as employees' use of their own personal smart phones is improving enterprise mobility, many popular collaboration tools and technologies are making it easier for individuals and groups to manage external electronic interaction. But today, popular tools like Skype create risks to resources behind the Motorola corporate firewall. E-zones free employees to take advantage of emerging productivity tools to capitalize on opportunities for open innovation without putting enterprise data at risk.



architecture will allow users greater access to network resources inside and outside the enterprise without the roadblock of today's inefficient access control and provisioning methods. When security is moved to end-user systems and to the data itself, users have the greatest chance of working on the network in an open collaborative way.

Jericho - the Walls Come Tumbling Down at BP

Some of the leaders in the IT industry have come together in the Jericho Forum to work on standards and best practices for the "de-perimeterization" of enterprise networks. Jericho members believe that perimeters and related existing security approaches are a barrier to change. Accordingly, they feel that perimeter firewalls will soon be displaced by emerging security methods that protect end-user computers and applications directly without the need for intervening perimeters, firewalls and expensive network-based tools. Central to this new paradigm is the idea that all end systems must be able to keep themselves secure on an untrusted network.

If successful, the Jericho approach will enable open and flexible internet-style connectivity within and between enterprises. Goldman Sachs, Boeing, Pfizer, Procter and Gamble, Barclays Bank, British Petroleum and Eli Lilly are a few of the companies who subscribe to the Jericho Forum's model of boundary-less security.

British Petroleum (BP) is a particularly good example of the direction that an E-zone architecture could progress. BP has moved 18,000 of its employee computers from behind the firewall and directly onto the Internet, using personal firewalls and other protections that are located on the end systems themselves. The theory is that corporate firewalls impede connectivity without adequately protecting end systems. The solution: simply harden end

systems and put them directly on the internet. The advantages to BP end-users are evidently substantial, because the company has measured the financial benefits of this approach and is continuing down the de-perimeterization path.

With the E-zone architecture, it is possible to use nested zones to achieve BP-style open networking for some data and applications. These zones would still protect Data of Concern with firewalls and other network based tools. Consequently, E-zones are an ideal platform for a gradual move towards the future state of borderless network access and protection.

CONCLUSION

E-zones Represent the Right Balance of Protection and Connectivity

The Motorola E-zones Architecture will empower business managers to find the right balance of network protection and network connectivity for their applications and digital assets. Consequently E-zones are an optimal solution to the growing drawbacks of Motorola's current corporate firewall perimeter. E-zones are designed to enforce compliance and manage risk by using proven methods like defense-in-depth for Data of Concern and a hierarchical policy framework.

Moving forward, E-zones are an ideal proving ground for IRM, IAM, and de-perimeterization. Ultimately, they will pave the way to the highly open forms of networking and seamless mobility of the future. Finally, zones will make it possible for Motorola business managers to use robust and resilient network connectivity to create the kind of dynamic knowledge sharing fabrics that will be necessary to respond to competitive pressures from all parts of the globe.

