Policy-Based Collaboration: Moving to an Enterprisewide Framework for Working and Communicating with Confidence

What You Will Learn

The business world is changing rapidly. As we move from many isolated regional economies to one global, interconnected economy, speed and agility are crucial. Organizations are rapidly transitioning from physical meetings to virtual ones, using rich online tools that enable workers to reach across geographies and time zones. People are collaborating with colleagues, partners, suppliers, and customers to reduce costs, use the knowledgebase to make faster decisions, boost productivity, accelerate innovation, and gain a time-to-market advantage. With the ubiquity of broadband, technology has evolved as the critical enabler behind these transitions. Workers are going mobile because they have the devices and networks to do so. The rise of service-oriented architecture (SOA) means support for a faster pace of software innovation, and the growing adoption of software-as-a-service (SaaS) will make these solutions available to a significantly broader base of the world's knowledge workers.

This relentless push to accomplish everything faster, better, and cheaper is motivating companies in all industries and of all sizes to embed collaboration capabilities into business processes and workflows that extend to both internal and external stakeholders. Businesses are recognizing that the capability to effectively include customers, partners, suppliers, manufacturers, and other external parties in their processes can lead to faster time to market, shorter sales cycles, increased productivity across entire workflows, and improved customer loyalty and satisfaction. But these benefits do not come without risks. While the Internet has made it possible to transparently share data and resources among widely dispersed groups, it has also paved the way for hackers to intercept that same data on the way to its intended destination, or exploit weaknesses in collaboration channels to gain unauthorized access to sensitive data and network resources. Anyone who wants to collaborate online must be concerned about this problem because, for most organizations, information is their most valuable asset and the lifeline of their business.

A truly effective, policy-based collaboration solution delivers the freedom for real-time collaboration with anyone at any time and the asynchronous sharing of structured or unstructured content, wherever that content may exist. Using a rich policy framework, the network is effectively able to differentiate between the contextual attributes of various users and resources to make precise decisions about what information users can access and how they can participate in online collaborative workspaces.

This document discusses the evolution of collaboration, the current state of on-premises and on-demand interaction, and why a policy-based approach is the key to securing cross-company communication and meeting regulatory compliance requirements. This document also examines how Cisco is uniquely positioned in the industry to address this challenge for our customers and make collaboration with confidence a reality over any network, on any device. This vision of policy-based collaboration delivers the best of both worlds: meeting the strictest IT security and

compliance requirements while enabling users to customize and personalize their workspaces, much as they have done with their personal and social spaces on the web.

Introduction

The Internet and availability of high bandwidth have created an always-connected, on-demand world, laying the groundwork for a globally cooperative communication environment. But most business collaboration is not taking place in person or among people together in the same room. Thanks to increasingly sophisticated IP networks, applications, and endpoints, it is instead being conducted using voice over IP (VoIP), web and audio conferencing, email, instant messaging, mobility, and video. This virtualized capability to work together has accelerated the pace of business and yielded significant business benefits: connecting a diverse workforce, enhancing mobility and innovation, improving productivity, reducing costs, and increasing time to market and to profitability.

Collaboration has completely redefined the global competitive landscape. Having the tools to interact with crucial business partners, especially for medium-sized businesses, may be the differentiator that delivers a competitive edge, particularly in comparison to large global corporations, which may be hampered by an inability to make quick decisions and take fast action.

In addition, more than ever before, corporate growth depends on gaining increased access to new customers, improving existing relationships, establishing new markets, and unlocking new business models. Globalization means companies must compete in more places while employing an increasingly mobile and dispersed workforce. Although the tools for remote collaboration are becoming ubiquitous, the security policies and technology required to protect that shared information are not always properly implemented, putting companies at quantifiable legal and financial risk.

Why Is Collaboration Crucial to Enterprise Success?

By connecting a diverse workforce and providing the tools to interact with crucial business partners, collaboration has become crucial to businesses wanting to grow rapidly and remain competitive. For example, sales professionals improve their performance by building relationships that generate incremental volume with existing customers, acquiring new customers, developing new channels, and closing bigger deals faster. Sales teams need to use every tool available to win customers, and they cannot wait while companies perfect their collaborative processes. If they cannot secure their communications, they will share information anyway and hope for the best. These are the real-life problems that policy-based collaboration can address. Rather than wait until critical data is compromised, organizations can now put policies in place to control and manage information on their networks and devices.

Companies that do business over the web are also taking advantage of collaboration. For many web-based organizations selling competing goods or services, customer service is often a primary differentiator. When customer service problems arise, the speed at which the situation is resolved is critical to retaining business. An unhappy customer will not care that a file could not cross a firewall because someone set up an incompatible policy. Customer service illustrates the need for collaborative security measures that not only protect intellectual property but also enable business, or they will create more problems than they solve.

Today, the tools to meet these challenges are increasingly common components of the corporate communication tool set. The strategic use of real-time collaboration can deliver the benefits of

increased productivity, compressed decision making, faster time to market, access to experts anywhere at any time, and enhanced customer and supplier loyalty. All these factors result in potentially greater growth and profitability and position policy-based collaboration as a foundation for the global economy.

As networks continue to extend far beyond physical organizations, security and privacy, information integrity, quality of service (QoS), accessibility, and reliability will play an increasingly vital role in enabling secure collaboration for businesses and their ecosystems.

Challenges of Collaboration

In a truly borderless enterprise, a policy-based collaboration platform can deliver a premium user experience that enhances every aspect of the business. Converged networks can carry critical information to and from remote workers inside and outside the traditional network perimeter to independent contractors, to their supply chains and customers, and into the larger partner ecosystem. But the convergence of these communication vehicles onto a single, secure platform is still a formidable challenge. For example, older equipment and applications from many different vendors must be networked, data in isolated locations must be accessed, and everything must be hidden behind an easy-to-use interface that requires little or no user training.

However, without strong corporate policies and a comprehensive policy-management solution in place, an organization's most valuable asset -- its information -- can be compromised. According to the Identity Theft Resource Center (ITRC), 127 million data records were exposed during 2007. This type of exposure can be very costly to the enterprise. A survey conducted by the Ponemon Institute, an independent privacy-management research firm, reported that the average data breach cost U.S. businesses $197 per individual data record in 2007.

Protecting priceless business assets, both on premises and over electronic networks, and avoiding single points of failure require a comprehensive policy-based architecture. A solution that dynamically profiles behavior can offer additional granular access control across the infrastructure.

A Strong Policy Approach to Security Concerns

Today's business environment includes an array of compliance requirements that are extremely complex and varied across different jurisdictions. By integrating traditional perimeter security with a more intricate strategy for collaborative technologies, organizations can effectively address the security and privacy requirements contained in Sarbanes-Oxley, Gramm-Leach-Bliley (GLB), the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) Data Security Standard, European Basel II, and other mandates.

Even with perimeter security and a strategy for collaborative technologies in place, networks may still be vulnerable. For example, cross-vector attacks, which exploit the weakest link in a unified communications infrastructure, may be launched against other parts of a networked environment. Hackers often target mobile handheld devices to circumvent stronger security placed on other computing devices, such as laptop computers. To protect mobile devices from cross-vector attacks and other potential threats, organizations must integrate wireless security policies into their larger security policy strategy.

Integrating security policies, helping ensure compliance and protecting valuable corporate assets, is only one part of a secure collaboration strategy. To achieve confident collaboration and help ensure data integrity and resource availability, organizations must effectively manage users'

access to data and the data itself. Identity management tools help organizations manage users, groups, roles, and attributes. For example, identity management tools can be used to restrict access to specific data based on a user's role in an organization. Similarly, data classification tools help IT leaders at enterprises understand the types and value of information moving across collaboration channels, so they can determine which users, groups, and roles can access the data. Both identity management and data classification tools need to work alongside and, where possible, be integrated into the policy-management infrastructure to enhance the capability of the enterprise network to serve as the secure platform for collaboration.

Cross-Industry Scenarios that Benefit from a Policy-Based Strategy

If collaboration and network-level security are critical to business, then so are policy management and enforcement as part of the network fabric. From a practical standpoint, security features must be standards-based, simple to administer, transparently integrated into the collaboration platform, cost-effective to deploy and manage, collaborative between technologies and platforms, and extensible enough to fit the specific needs of each company. At the same time, organizations must enforce policy management from a business perspective by defining goals, roles, and patterns of usage across all applications, including data, VoIP, instant messaging and presence, web, collaborative workspaces, and audio and video conferencing.

The following scenarios provide examples of how policy-based strategies can be implemented to help deliver tangible business benefits. They also illustrate the disastrous potential of unintentional security breaches due to a lack of comprehensive policies.

Financial Services

In the investment banking business, professionals often share information with colleagues while it is in the process of being incorporated into formal and complete documents. In this scenario, a financial analyst decides to share a draft research report on the pharmaceutical industry to collect feedback and help ensure factual accuracy. She attempts to call a colleague to review the draft report. Unknown to her, the colleague recently changed jobs and is now a broker in the same firm, selling pharmaceutical stocks to institutional investors. Her organization's strong policy-management framework automatically blocks the call because of his new job function. She tries to contact the colleague by email and instant messaging, but they are also blocked. If this policy had not been enforced, the firm would have violated a critical SEC rule governing ethical walls, resulting in heavy fines for the firm. This example is a clear illustration of an ethical employee potentially violating a very serious policy without any malicious intent. Fortunately, the strong policy and governance framework prevented this inadvertent communication and saved the firm potentially millions of dollars in fines.

Oil and Gas

Oil exploration is extremely expensive and risky, so companies often share the costs of drilling new oil wells by forming joint ventures. Each participant may contribute intellectual property about the drilling site, drilling methodologies, and other technical know-how. Because the companies involved also compete with one another, it is crucial that only authorized people who are involved with the joint venture and who have signed strict confidentiality agreements are granted access to the collaboration site. Without a policy system governing access or entitlements to these sensitive documents and content, this partnership could fail, because each company would likely refuse to share much of its knowledge because of competitive concerns. However, a strong policy-based architecture helps ensure that only those with the proper job role can access sensitive data, and

only within the right context and conditions. For example, the policy system may block access to the collaboration site if the user is accessing it over a public Wi-Fi network. With these policy controls in place, the project can proceed.

Government

Governments, both national and state, may need to release information to only a few trusted compatriots. In this scenario, the U.S. government compiles a terrorist threat database that it shares selectively with other countries. After recent bombings, India's government requests access to the database to compare it against its own intelligence reports. The information is highly sensitive and could compromise national security, so the U.S. government is apprehensive about sharing it. But because India is an ally, the U.S. government decides to offer selected records for a fixed period of time and to only a few named individuals in India's top intelligence agency. A policy-management system helps ensure this very limited level of disclosure and access by enforcing access controls over who can access the information, how it can be used, and how long it is available.

Optimizing Collaboration Through Enforceable Policy Management

The policy-directed technologies called for in the preceding financial services, oil and gas, and government scenarios already exist. All that remains is to bring them together in a comprehensive platform. The Cisco vision is to optimize collaboration with a solution that encompasses the entire enterprise, including internal and external data sources. This solution automatically enforces security and governance policies while enabling business-to-business collaboration that delivers appropriate value from the data center to the desktop.

To help corporate IT administrators meet the security challenges of collaborative environments, Cisco engineers its collaboration platforms to the highest standards of safety and integrity. The following Cisco® secure collaboration solutions enhance business productivity and agility across the spectrum of applications, devices, networks, and operating systems.

Secure Infrastructure with Cisco TrustSec and Cisco IOS Software

A secure infrastructure is the fundamental building block for a secure collaborative environment. Maintaining high availability (QoS, etc.) and dynamic access management (VLANs, etc.) enables secure collaboration, and dynamic tagging of devices and data packets helps ensure that security policy is enforced across the entire network. These benefits can be achieved using an organization's existing IT investment and adopting Cisco TrustSec, a new architecture that delivers scalable switch security services through:

- Secure campus access control: Provides consistent role-based identity and controlled access to critical applications and resources
- Converged policy framework: Converges the various roles, servers, and access definitions and simplifies the management of identity policies
- Pervasive integrity and confidentiality: Safeguards against data leakage in support of regulatory requirements

Cisco routers also provide robust and adaptable security solutions that help defend against denial-of-service (DoS) attacks and other threats to the network infrastructure. Cisco IOS® Software on routers offers a comprehensive suite of security technologies such as Cisco IOS Firewall, Intrusion

Prevention System (IPS), IP Security (IPsec), and Secure Sockets Layer (SSL) VPN. These technologies provide the following benefits:

- Additional protection without deploying new hardware: Enable new security features on existing routers using Cisco IOS Software.
- Increased security where companies need it most: Apply security functions, such as firewall and IPS, as well as centralized device and policy management, anywhere in the network, including remote branch offices.
- Savings of time and money: Reduce the total number of devices in a network, thereby decreasing ongoing support and manageability costs.

Cisco Data Loss Prevention Solutions

A crucial concern related to collaboration is the increased amount of traffic traversing the network perimeter. Cisco data loss solutions are designed to maintain regulatory compliance and data integrity by:

- Authenticating users and devices before permitting network access (using Cisco Network Admission Control [NAC])
- Providing a real-time inventory of sensitive or confidential information stored on endpoint devices, and security to prevent that information from inadvertently being sent to unauthorized users or loaded onto removable media (using Cisco Security Agent)
- Filtering email to help ensure that confidential information is not passed along through email (using Cisco IronPort® technology)

Cisco WebEx Connect

Many aspects and layers of security features in Cisco WebEx® Connect are designed to protect corporate and personal data, prevent unauthorized access, and preserve business-sensitive information. Cisco achieves the highest level of security for its Cisco WebEx Connect customers by employing industry-standard best practices in physical site, application, and network security. Cisco WebEx Connect can also use Cisco Enterprise Policy Manager, a leading entitlement and policy-management product that Cisco gained as a result of the Securent acquisition in late 2007.

The Cisco WebEx Connect collaboration platform meets the requirements of a truly effective policy-based collaboration solution by providing a rich policy engine that can account for a variety of attributes, such as user roles, resources, time of day, network location, device health, project ID, and any number of attributes to make precise policy decisions. Cisco WebEx Connect also offers flexible policy modeling and delegation to appropriate administrators, allowing them to tightly control network and content access by setting security policies that map to business processes. In addition, Cisco WebEx Connect delivers:

- Integration with heterogeneous enterprise collaboration and messaging products, without the need for any additional third-party products, which is critical to providing enhanced productivity
- Robust performance and reliability, which require a multilayered approach and elimination of all single points of failure through full redundancy of all system components
- Granular logging of all events, including end-user actions and administrator transactions, which is vital to helping ensure security and compliance

- An extensible platform that brings together instant messaging and audio, video, and web conferencing, enhancing asynchronous collaboration and helping companies keep up with the changing business needs of their users

Cisco Enterprise Policy Manager

In order to achieve the goals outlined in this paper, each organization must deploy a robust enterprise policy-management platform that is integrated with their unified communications and collaboration solutions. Cisco Enterprise Policy Manager (EPM) provides rich, granular entitlement management functions for a broad set of enterprise applications and data stores, including Cisco Unified Communications products and Cisco WebEx Connect. Cisco EPM can be used to manage policies governing whether a user can access a document, view a report, perform a transaction, join a chat session, or communicate with another person. By externalizing policies and managing entitlements outside of each application silo, organizations can apply these policies consistently across heterogeneous applications and have a central point for administration and audit.

Clientless SSL VPN

Clientless SSL VPN allows remote users to access corporate resources from essentially any location or device, whether on the road or at a trade show kiosk. The clientless SSL VPN can also dynamically limit access based on user authentication, making it an ideal solution for contractors or guest users who need network access, who cannot install a client, and who need access to only a predetermined set of applications or resources.

Cisco Secure Desktop

Cisco Secure Desktop works with the SSL VPN solution to create a virtual desktop on any endpoint machine. It provides impromptu conversion of thousands of non-HTML applications so they can function in an HTML web browser and supports latency-sensitive applications to create a LAN-like experience in a completely secure work environment.

Cisco ASA Adaptive Security Appliances Phone Proxy

Cisco ASA Adaptive Security Appliances Phone Proxy enables casual teleworkers to plug Cisco IP Phones into their home networks and use the native encryption of the phones to create secure connections back to the corporate network. This capability extends the in-office experience to remote workers by providing integrated communications tools to enhance teleworker productivity and collaboration. The Cisco ASA Phone Proxy can authenticate the device, terminate the encrypted connection, tie the phone into the internal phone network, and encrypt and decrypt the connection between the encrypted remote phone and the unencrypted phone network inside the internal network. These actions are accomplished while providing the QoS necessary to maintain the latency-sensitive bandwidth required for voice connections. In addition, the Cisco ASA Phone Proxy provides in-network services and productivity to remote users without the need to deploy additional routers or VPN devices at the home office.

Cisco ASA Presence Federation

The Cisco ASA Presence Federation creates secure connections between Cisco and Microsoft Presence Servers for secure collaboration between companies.

Cisco ASA Mobility Proxy

The Cisco ASA Mobility Proxy allows a wide range of mobile devices to be securely connected to the internal network.

Cisco Virtual Office

Enhancing the tools available to remote workers enables greater collaboration between them and the centralized workforce. The Cisco Virtual Office solution combines products, technology, and services to provide secure, rich, and manageable network services to teleworkers and employees at remote locations. The components of the solution include a remote site presence, a headend presence, a set of management capabilities, and services that facilitate deployment and ongoing maintenance.

Cisco Virtual Office offers flexibility and enhances productivity for users at their home or remote offices by providing office-caliber data, wireless, voice, video, and TelePresence services. By providing these capabilities with robust security, Cisco gives users the flexibility of managing their schedules while working from home. This solution is maintained through an automated zero-touch deployment model, which dramatically improves the efficiency of IT departments by saving time and reducing costs. The Cisco Virtual Office solution improves the productivity of businesses by empowering the workforce wherever it is located.

Collaborate with Confidence

Collaboration offers organizations opportunities to enhance productivity, accelerate innovation, and gain a competitive advantage. As organizations, forms of communication, and networks continue to evolve, the need to create a more dynamic and secure infrastructure to enable collaboration will grow exponentially. With this in mind, Cisco has identified the main steps through which organizations can enable their internal and external stakeholders to collaborate with confidence:

Step 1. Identify Collaboration Ecosystem

To achieve collaboration with confidence, enterprises need a collaboration ecosystem that enables interaction from anywhere to anywhere, connecting on-premises groups with others across the Internet. This step enables improved business-to-business collaboration, with users on both sides of the firewall able to communicate without having to worry about security breaches or compliance. To get started, organizations need to clearly define their objectives for collaboration, including the scope of the solutions and the technologies to be supported, as well as a flexible, future-looking strategy that allows refinement and growth as needs and technologies evolve. This approach will allow organizations to remain competitive while avoiding the need to replace expensive devices or solutions that cannot meet future security and collaboration requirements.

Step 2. Define Policies

The next step is definition of the policy-defined borderless enterprise, where anyone can collaborate with confidence, sharing information in context and thus accelerating business innovation. The network in this environment will enable secure, trusted communities through tight interaction between foundational network security and collaboration-enabled security appliances. This approach relies on the ubiquitous deployment of corporate policies that enable the dynamic, personalized definition of behaviors, along with enforcement of compliance with those policies. To enhance the secure deployment of collaboration tools within this borderless environment, policies need to be integrated into the larger corporate security and network policies; doing so helps ensure that existing policies do not inadvertently limit the ability to deploy new collaboration solutions, and conversely, that these new collaboration tools do not introduce new risks to the enterprise that are not covered by the foundational security and network policies.

Step 3. Create a Collaborative Culture

The changing nature of the enterprise has led to more telecommuters, remote offices, and traveling workers. With more employees in more places, services and storage must be made available wherever and whenever they are needed. Collaboration in this environment will move into the home and on the road and will require integration between intelligent remote and network security technologies and a broadening range of network and collaboration services. This integrated approach will enable both policy-controlled access and deep traffic inspection regardless of where communications originate or the devices or access methods employed.

Among the main technologies that enable this vision are resource allocation and management, which help ensure that the network can deliver a rich collaboration experience to the appropriate users without consuming all available bandwidth. In an environment that supports a collaborative culture, policy-based solutions will act as gatekeepers, modifying users' behavior without denying access to those who need it.

Conclusion

Unified communications, along with the collaboration it enables, has become more than an efficiency tool; it is a strategy that is a primary concern of enterprise executives. Organizations that most effectively adopt and employ these technologies will be able to move faster and differentiate themselves in today's competitive environment.

The best solutions that achieve this level of secure collaboration require a comprehensive policy-based architecture that dynamically profiles behavior and offers granular access control at the network level. This approach addresses compliance concerns and allows users and enterprises alike to collaborate with confidence from anywhere, with anyone, at any time, and on any device.

At Cisco, we understand the needs of employees who collaborate both on corporate premises and remotely, as well as those working on hosted, web-based platforms. Cisco aims to provide a common platform that delivers the appropriate level of security and QoS for each unique interaction. By enabling the creation of secure collaborative environments, Cisco is truly accelerating the way business works and freeing organizations to share, motivate, innovate, cooperate, and conduct all their transactions without risk, enabling secure collaboration with confidence.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-497588-00 11/08