White Paper

The Policy Governed Network

A New Enterprise Architecture for Delivering Policy-Based Services

What You Will Learn

This document discusses the need for a policy-based architecture in today's enterprise networks and presents Policy Governed Network architecture as a pragmatic business solution. Building identity and context awareness into the network is critical to implementing an effective infrastructure. Major topics include:

- What policies are and who implements them
- Changing network dynamics and problematic new technologies
- Important challenges to implementers
- Characteristics of a Policy Governed Network architecture
- Policy-implementation platform: the Cisco® Identity Services Engine
- Scenarios showing how policies can address specific network issues
- How to begin transitioning to a Policy Governed Network

Why a Policy-Guided Approach Is Essential

In the past few years a number of paradigm shifts have made policy-based networking essential to effective enterprise IT management. These shifts include an increased reliance on virtualization, cloud computing, and software-as-a-service (SaaS) applications; the "consumerization" of business networks that has occurred with the popularity of devices such as tablets and smartphones; and the rapid adoption of video in business communications. By applying appropriate policies within the network, IT managers can do a better job of meeting users' expectations and aligning service delivery with business objectives.

A policy-based networking approach helps IT staff to accomplish business goals such as the following:

- Give authorized users access to sensitive data when they are in certain locations or using specific devices, while restricting access from other locations or from other devices. For example, a policy might permit a finance manager to access data from anywhere using a company laptop, but restrict the manager's access to a specific resource from a personal device outside the office.
- Route all traffic from point-of-sale systems in branch locations using encryption and a guaranteed quality of service (QoS). Other traffic from the branch might remain unencrypted and receive less priority.
- Prioritize multimedia telepresence calls with customers during peak network traffic periods, while assigning lower quality of service or best-effort status to nonbusiness video originating on the web.
- Increase employees' productivity when they travel between cities by dynamically provisioning virtual desktops in the company data center closest to them.
- Block employee access to nonbusiness social networking sites during business hours, and block contractor access to such sites at all times.

Enforcing business policies using the tools available today has been challenging for IT organizations. The primary obstacles include the lack of effective tools, the difficulty of obtaining consistent device information, the need to coordinate across diverse teams and tools, and the absence of system-wide visibility. To solve these challenges, IT managers must start by building identity and context awareness into the network itself. This awareness will help them to define and enforce the business policies governing the networks.

The Cisco architecture for achieving a policy-based networking infrastructure is called Policy Governed Networks. The first step in making this architecture a reality is implementing Cisco Identity Services Engine (ISE), a core technology that delivers business-critical services by building and enforcing identity-and context-based policies for users and devices.

The Policy Governed Network: An Architecture for the Future

- A Policy Governed Network allows enterprises to define policies based on business objects and deliver policy-enabled services across on-premises, cloud, and SaaS applications. These business objects incorporate real-time information about users, devices, locations, applications, and services, among other attributes.
- A Policy Governed Network lets business managers define business-critical policies based on business objects for “anytime, anywhere” access to applications.
- A Policy Governed Network gives business managers consistent visibility into network activity, allowing them to measure service levels and adjust policies to meet desired levels.
- A Policy Governed Network provides a central location for defining policies, tracking activity, and enforcing the policies, enabling managers to measure compliance to regulations and identify compliance gaps.
- The Cisco Identity Services Engine offers the first step in implementing a Policy Governed Network by providing visibility, enforcing identity-based access policies, and protecting critical data throughout the network.

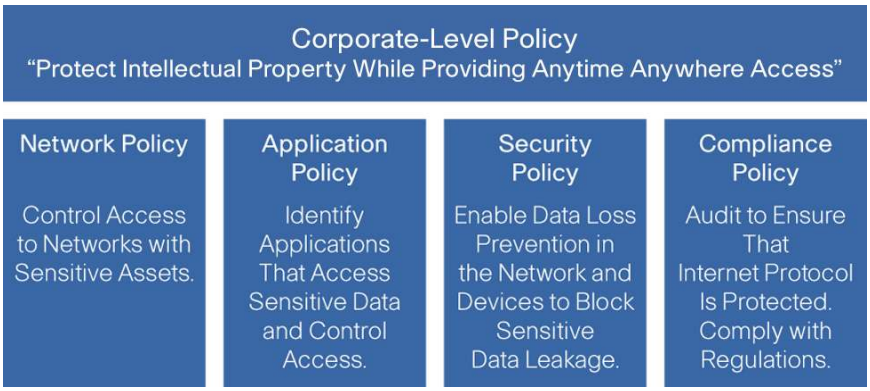
Anatomy of a Policy

A policy is broadly defined as “a definite course or method of action, to guide and determine both present and future decisions.” Today, network policies not only address access and security, but also applications, regulation compliance, and other issues crucial to business practice. From a chief information officer (CIO) perspective, an enterprise network policy should:

- State what should be done, but not focus on how it should be done
- Operate so it requires no manual translation
- Operate so it can be audited, and its effectiveness measured and adjusted if necessary

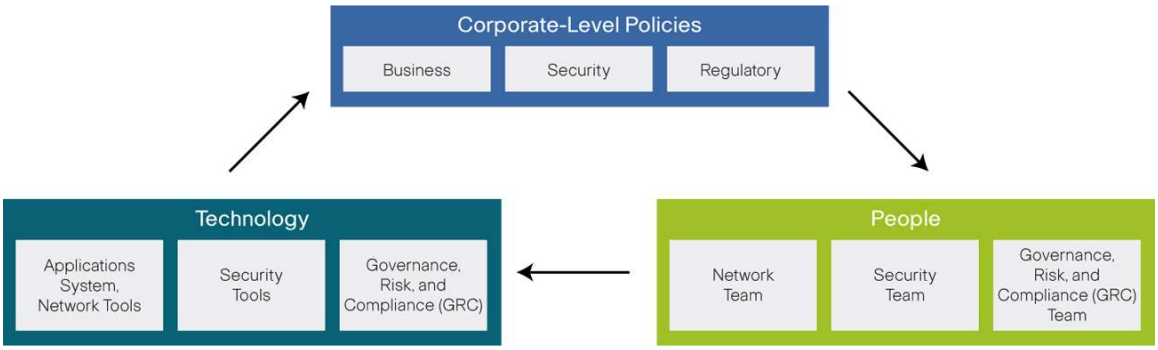
The CIO defines and oversees corporate-level IT policies, and makes sure they align with strategic business objectives. Various IT teams may define and carry out subordinate policies associated with a corporate-level policy, as shown in Figure 1.

Figure 1. A Policy Hierarchy



The different teams implement their policies using the IT tools available to them. Figure 2 summarizes the elements involved in defining and implementing a policy.

Figure 2. Elements of a Policy



Changing Network Dynamics

Policies are playing a more central role in IT because several dynamics have changed in business networking. Policies based on a more detailed view of identity and context throughout the organization are needed to address disruptive network trends such as cloud computing, consumerized mobile devices, and burgeoning video traffic.

- **Cloud computing, virtualization, and SaaS:** A Savvis survey of 172 chief technology officers (CTOs) and IT managers released in November 2010 revealed that 75 percent were employing enterprise-class cloud technology or planned to over the next five years. IT research firm Gartner reported that cloud computing was their most popular topic of inquiry in 2010. With cloud-based computing, the end user often has no knowledge of where the computation takes place and where applications and storage reside. With desktop virtualization, traditional data center elements must be as transient as the mobile workers who use them. And with adoption of the software-as-a-service paradigm, business-critical applications must be accessible from anywhere over secure connections. All this requires policies that allow IT staff to effectively implement and manage access and security measures as users constantly migrate and virtual machines are created, moved, and recreated.

- **Consumerization and mobility:** According to the Cisco Visual Networking Index (February 1, 2011), an ongoing project to forecast the impact of specific technologies on networks, global mobile data traffic grew 2.6-fold in 2010, nearly tripling for the third year in a row. The index estimates that there will be 788 million mobile-only Internet users by 2015. Users are increasingly reliant on smartphones, tablet computers, netpads, and other mobile devices that can now be equipped with enterprise-level capabilities. To maximize these capabilities and enhance productivity, IT must be able to give consistent access to any enterprise resource from any location across both wired and wireless networks. Policies must be able to accommodate these devices and keep up with the innovations that the workforce may already be using in their personal lives and want to carry over to their work.
- **Video-oriented applications:** IT organizations are constantly rolling out new, more demanding services across the network infrastructure. A chief example is video. According to Cisco's Connected Technology World Report the rise of video in the workplace is real. Globally, more than two-thirds of IT professionals (68 percent) feel that the importance of video communications to their company will increase in the future. Companies spent $2.2. billion on video conferencing and telepresence technology in 2010, according to Infonetics Research. With mobile devices equipped with high-definition video in the hands of users, bandwidth consumption is quickly becoming a vexing issue for IT. Managers will need to put policies in place to prioritize this traffic and help ensure the service quality that video requires. In addition, enterprises and service providers also wish to meter video services, and specific policies will be needed to support this and other changing business models.

Policies are becoming more nuanced as a result of increased heterogeneity and complexity within organizations and their networks. This trend has resulted in increasingly sophisticated network policy enforcement requirements. There are a number of challenges to implementing effective policies in current enterprise environments.

Challenges Facing Policy Implementers

The most important challenges that organizations face while implementing policies are aligning the policies with business requirements, coping with poor operational visibility, providing effective service delivery, and adapting to changing conditions and technologies.

Aligning Policies to Business Goals

It is not an easy matter to express policies in terms that are meaningful to a business. Nor is it simple to enforce such policies while also taking into account a profusion of user identities, roles, devices, applications, services, and locations. In today's networks, concepts such as user, device, and service are not fixed and constant, making it more difficult to define and enforce policies that accurately reflect business goals.

Because identities are often distributed across multiple directories and databases, there is no dynamic and comprehensive source for identity information. Active Directories usually only store employee accounts, not information on business partners, contractors, customers, or other entities who may need access. Similarly, there is no central resource for device and asset information, because device information is spread across different teams and different systems. As a result, organizations have no choice but to manually translate business policies into the underlying technical language that the infrastructure recognizes, which is largely limited to IP addresses, media access control (MAC) addresses, access control lists (ACLs), device ports, and protocols.

In addition, the inability to create and enforce policies based on identity makes it harder to enforce service prioritization in a way that does not compromise employee productivity and that minimizes nonessential application usage.

Coping with Poor Operational Visibility

Another important challenge facing IT managers is their inability to achieve adequate visibility across the infrastructure so that they can correlate information. For example, consider this policy use case: “Restrict outside-the-office access to certain applications from personal devices such as Apple iPads to ensure compliance with Payment Card Industry (PCI) security standards.” This policy is impossible to implement if there is no straightforward way to identify iPad users and correlate them to particular PCI-relevant applications.

Currently, full network visibility is limited by the fact that responsibility for assets and reporting is divided among several different entities.

- Application teams provide application usage reports consisting of users and the resources accessed.
- Systems teams provide system usage reports focusing on the Unix IDs of those users accessing the system. These users are generally different from application users.
- Network managers provide network utilization reports derived from traditional network management tools, and usage reports based on physical networks and virtual LANs (VLANs).
- Security teams provide access control reports based on networks, VLANs, the IP addresses accessing the network, and PCI-oriented applications.

IT and business managers find it very difficult to correlate these diverse reports because there are a host of inconsistencies among users, devices, networks, IP addresses, and application resources. Auditing for regulation compliance therefore becomes a time-consuming manual task.

Furthermore, device information is spread across many systems, such as asset databases and device and patch management systems. There is no meaningful source for location or presence information except for the information that is based on IP address or VLANs. Not having this contextual information makes it difficult to differentiate, for example, between an authorized user of a corporate device within the office and a user of a personal device outside the office.

Ensuring Effective Service Delivery

One consequence of the lack of real-time user, device, and service awareness is that organizations do not have the ability to make effective policy-enforcement decisions. For instance, business-critical functions at branch locations such as point-of-sale (POS) terminal communications and IP-based surveillance videos need to be given a higher priority than other services to ensure business continuity and safety. However, because there is no consistent view of users, devices, and services, businesses cannot dynamically prioritize and adjust services based on current branch WAN link utilization. Instead, the network services are confined to a static configuration without any customization or personalization. This means that critical business services may suffer during periods of peak network traffic.

Adapting to Changing Needs

The virtualization of data center resources, while beneficial in terms of efficient use of valuable physical resources, is placing enormous demands on the network and operations teams. Consider the case of dynamically provisioning an employee virtual desktop in the closest data center when that employee travels from the London office to the New York office. Traditional tools today are not flexible enough to move virtual machines or their profiles closer to the employee. Nor do they have the agility to take account of available resources in the closest data center, and to make sure that compliance policies are not being violated and that service-level agreements are being met. This leads to inefficient changes to implementation, reducing the dynamic nature of virtual services and making users less productive and data assets more vulnerable.

Solution: The Policy Governed Network

The solution that allows managers to overcome these challenges starts with using identity and service knowledge embedded in the network. This lets IT managers define and enforce business-relevant policies efficiently. Cisco calls this comprehensive approach a Policy Governed Network. Table 1 outlines the resulting benefits.

Table 1. Policy Governed Network Benefits

Stakeholders	Benefits
End user	Increased productivity Personalized, predictable experience Assured security
Administrator	Central location for definition of policies Real-time awareness and dynamic enforcement Ability to adjust policies to meet desired service levels
Auditors	Consistent visibility of activity and auditable enforcement of policies Ability to measure regulation compliance
CIO and business managers	Consistent business-relevant policies, aligned with business objectives Regulatory and security compliance System-wide visibility and control

Effective policy implementation requires context awareness, which comes from a consistent, real-time view of users, devices, and services within the infrastructure. Managers can use this information to dynamically enable services based on policy, improving the quality of the interaction for the end user and offering a more sophisticated, situation-aware, and personalized experience.

For example, consider a network that creates context by using a variety of information sources to determine that the vice president of sales is currently in a branch office location conducting a telepresence session with an important customer. The network senses that the WAN uplink for that branch is getting congested and automatically upgrades the quality of service for the telepresence session, while at the same time reducing bandwidth for nonessential or non-time-sensitive applications.

The Policy Governed Network provides real-time awareness and incorporates a more comprehensive set of dynamic context information, such as location, presence, and service usage. This helps the system to make intelligent, efficient policy-enforcement decisions. A Policy Governed Network also provides the ability to measure, monitor, and adjust the environment so it can adapt to changing conditions such as network availability and congestion, real-time security threats, and service migration. In addition, the architecture provides more visibility into who and what is on the network, simplifying compliance verification and audit procedures.

To effectively meet business objectives, IT organizations need a policy-based service platform that lets them deliver cross-domain application and network services in an agile, efficient, and secure manner. Cisco Identity Services Engine (ISE) provides a centralized policy platform designed to meet this need. Cisco ISE helps IT managers to fulfill productivity, security, and compliance requirements by building and enforcing identity-based access policies for users and devices, while protecting critical data throughout the network. The first release of Cisco ISE will support secure access scenarios, with future releases providing support for capabilities such as virtual desktop infrastructure, branch office service prioritization, and other major business-critical service implementations.

In response to the changes in the IT and threat landscape, Cisco developed the Cisco SecureX Architecture, which is specially designed for the Policy Governed Network. Cisco SecureX blends the power of the Cisco Policy Governed Network with context-aware security to protect today's organization no matter when, where or how people use the network. This architecture uses next-generation distributed granular scanning and inspection elements to enforce context-aware policies throughout the network and across a wide range of devices and services. Unlike conventional security solutions, SecureX operates with a much broader array of parameters and context. For example, it can determine the identity, location, and role of the person attempting access, as well as what sort of device that person is using. Instead of focusing on static endpoints, this security approach supports today's "any device, anywhere" work patterns while still safeguarding privacy or data. Security policies are managed centrally, but intelligence is gathered and enforced globally.

Policy Governed Network Architecture

An architectural approach to policies supports creation of multiple solutions that take advantage of the policy platform and integrate other products from various vendors and service providers. The Policy Governed Network architecture leverages standards wherever feasible, and provides the ability to integrate with other products and solutions to ease implementation. The architecture is flexible and scalable enough to support a consistent policy framework across multiple technology elements—including the ability to define, store, evaluate, aggregate, decide, enforce, and track policies.

Essential Characteristics of a Policy Governed Network

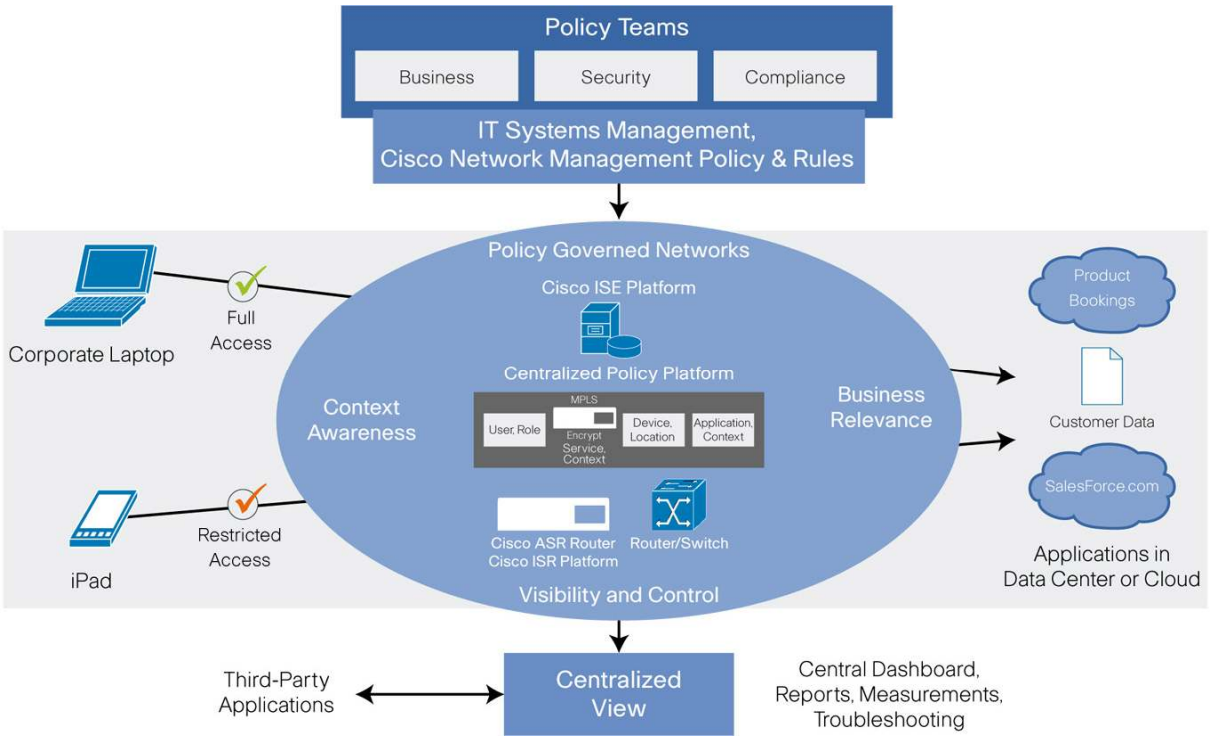
The Policy Governed Network provides context awareness of the user, device, and application being accessed. These constitute the business objects inside the policy platform. IT managers use these objects to define dynamic policies and enforce the policies in the infrastructure based on business context (such as employees, guests, device, country, or campus) instead of the static technical context (IP address, MAC address, or user ID).

Business objects consist of typical, everyday nouns used to express elements of a policy. For example:

- Users, such as employees with accounts in Active Directory, or guests who are temporarily granted network access
- Devices, such as endpoints that connect to the network: managed laptops, employee or contractor devices, tablets, printers, and scanners that can all be defined or discovered from the network
- Locations, such as inside the company office or at home, that are important for certain security and regulatory policies
- Applications, such as sensitive data residing in PCI or Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliant databases
- Time, such as during business hours or after hours

The values for the business objects are populated by gathering real-time information from the network infrastructure and by providing connectivity to various information sources so as to retrieve attributes of users, devices, and services. Typically, these sources of information are identity sources such as Active Directory, asset databases for devices, and location-based services (Figure 3).

Figure 3. Business Objects in a Policy Governed Network



With the abundant context available through business objects, IT managers will be able define dynamic policies that are relevant to business, instead of using only static technical configuration rules. Business, security, and compliance teams can define policies either in an existing IT systems management (ITSM) tool or in a Cisco solution. The Policy Governed Network architecture integrates with IT tools to ease the definition of the policies. In addition, the architecture integrates with various policy information sources such as identity management systems to obtain identity attributes.

Once the policies are defined, they are provisioned in the IT infrastructure. The Policy Governed Network will initially focus on provisioning the policies on Cisco devices. Cisco anticipates that these networks will eventually provide the necessary applications program interfaces (APIs) and connectors to integrate with application servers, other vendors' devices, and security software.

The Policy Governed Network also provides contextualized visibility and control of the "who, how, what, and when" for the identities (of users and devices) attempting to access services. Instead of having many static, uncorrelated reports from applications, networks, and systems, the Policy Governed Network acts as the source of contextualized data, empowering managers to assess the effectiveness of policies and alter them to meet changing business requirements. Additionally, the session directory is an excellent source for automating and measuring compliance with regulations and security policies. This provides significant benefit to the business by minimizing the manual activities involved with measuring compliance.

Policy Governed Networks in Action

The scenarios below offer examples of how a Policy Governed Network architecture can benefit enterprises by making networks more responsive to business models.

Scenario 1

Control access to regulated data based on user, device, and location. Deny user access to regulated data from iPads and grant access from a corporate laptop in a company location.

Joe, a finance manager, is accessing customer data from his company-issued laptop while in the office. Customer data is controlled by regulations, and access is based on clearance levels. Joe is allowed access to this information because he is part of the finance team and his entitlements, which are stored in Microsoft Active Directory, give him a right to this information.

Now suppose Joe tries to accesses the customer information from his corporate laptop while sitting in an airport lounge. Regulations state that he should not be allowed access because people sitting nearby might be able to see the information, or even photograph it. However, if Joe tries to access the protected information from his personal iPad, regulations would prevent access because security and data loss prevention (DLP) controls on the iPad cannot be ascertained.

With a Policy Governed Network, the organization can define the following business-relevant policies to enforce compliance with these regulations (Table 2).

Table 2. Scenario 1: Policy Definition

User	Role	Device	Service	Location	Action
All	Any	iPad	Product bookings	All	Restrict
All	Any	iPad	Salesforce.com	Out of Office	Allow
Any	Finance	Corporate asset	Product bookings	Office	Allow
Any	Finance	Corporate asset	Salesforce.com	Office	Allow

Table 3 outlines the situation before a Policy Governed Network was implemented, and afterwards.

Table 3. Scenario 1: Policy Governed Network, Before and After

Before	After
• **Application team:** Integrate user and device entitlement into the application to ensure appropriate access to data. This process is repeated for each different type of user and device. • **Network and security teams:** Define ACLs on firewalls allowing access to networks. • **IT manager:** Must view multiple usage reports from application, network, and security teams, each with different contexts for user and device, making it difficult to get contextualized visibility. • **Outcome:** Multiple teams configure static configurations in areas of applications, systems, networks, and security without a consistent context of user, device, or application.	• **Cisco Identity Services Engine:** Allows IT managers to define and evaluate policies • Network devices get the context of the policy and enforce it on the user traffic flow. • When a user connects to the network, Cisco ISE detects the user and, based on the device profile and the role of the user, provides access or denies access. • In the future, it is anticipated that Cisco ISE will integrate with applications to obtain the context of data sensitivity and enforce the policy as the user accesses applications containing sensitive data. • **IT manager:** Acquires a contextualized view offering visibility into user and device activity and policy enforcement. • **Outcome:** Automated policy-based management instead of manual coordination across many tools, helping the manager to apply a business-relevant policy with consistent context and the ability to measure and adjust the policy based on business needs.

The Policy Governed Network architecture will be able to match identity with real-time awareness to help ensure that the policies are enforced in the infrastructure. Figure 4 depicts how this works, and a contextualized report (Table 4) follows.

Figure 4. Scenario 1: Network Diagram

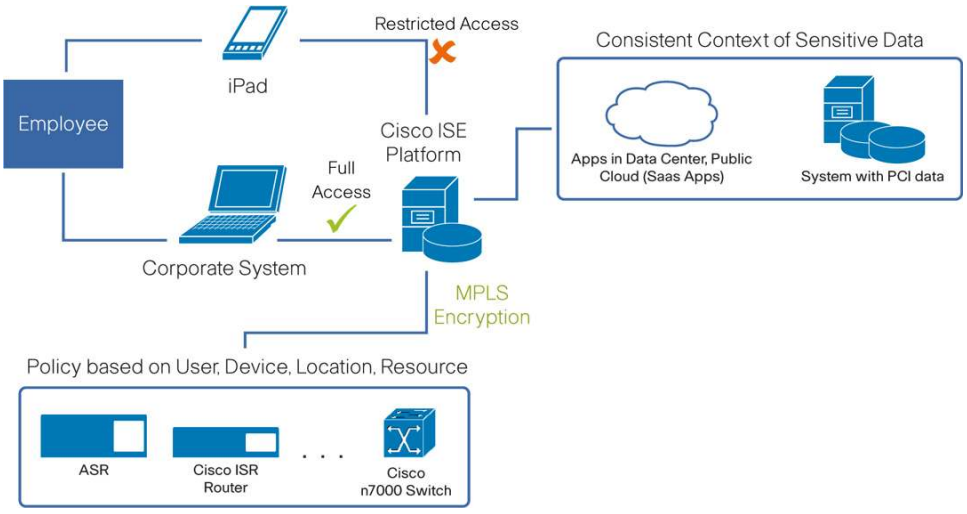


Table 4. Scenario 1: Contextualized Report

User	Device	Location	Resource	Action
Joe (role: finance manager)	Corporate laptop	San Jose campus, Building 1	SAP applications with customer data	Granted, time
Joe	iPad	San Jose campus, Building 1	SAP application	Denied, time
Joe	Corporate laptop	Seattle (coffee shop)	SAP application	Denied, time

Scenario 2

Provide service prioritization for a branch office. Prioritize access based on user, device, location, and service context. Allow iPads.

Joe, the finance manager, uses a virtual desktop. His desktop is actually a virtual machine located in the data center. Joe is engaged in a customer call, a teleconference session with video using Cisco WebEx® collaboration technology. Coworkers in the office can access YouTube and other non-work-related sites from their virtual desktops and local devices. From the same office, the general manager is conducting a telepresence session with a customer using Cisco TelePresence® technology. A WAN link between the headquarters location and branch location is becoming saturated with the high-volume traffic.

The challenge: Provide different levels of service based on user, device, and service contexts. These levels might be termed Platinum for the highest quality of service, Gold for next-highest priority, Silver, Bronze, and so on. Best-effort service is at the bottom of the hierarchy. The IT manager would like to create policies that can automatically manage the situation, as shown in Tables 5 and 6.

Table 5. Scenario 2: Policy Definition

Role	Device/Technology	Location	Service, Context	Action	Condition
All	iPad	Any	Cisco WebEx	Grant	Best effort

Sales manager	Virtual desktop	Campus, branch	Video	Grant	Bronze QoS
General manager	Cisco TelePresence	Branch	Customer session	Grant	Platinum QoS (1080-pixel resolution)

Table 6. Scenario 2: Policy Governed Network, Before and After

Before	After
• **Network teams:** Define QoS policies based on source and destination IP addresses and networks. • **Systems teams and virtualization teams:** define configurations using the tools to manage systems and virtualization. The context is based on user ID and the applications user can access. • **IT managers:** Lack visibility into policy enforcement, making it difficult to measure and adjust policy to meet business needs. • **Outcome:** Lack of context makes it difficult to define and enforce policies end to end with a consistent context.	• Polices as described above can be defined in Cisco ISE with a consistent context of user, device, application, and the type of service needed. • Cisco ISE detects the Cisco TelePresence device and participants in the session. • Polices are evaluated and downloaded to the network devices. In this case, the network devices download the policy and enforce it on the user traffic flow, providing the QoS level based on the user, device, and the participants in the TelePresence session. • As policies are defined and enforced with a consistent context, IT managers get visibility into the user, device, and activity, as well as the results of policy enforcement, allowing them to measure and adjust policies to meet business needs.

The Policy Governed Network architecture is able to connect identity to real-time awareness, helping ensure that the policies are enforced at the branch office for WAN link optimization (Figure 5 and Table 7).

Figure 5. Scenario 2: Network Diagram

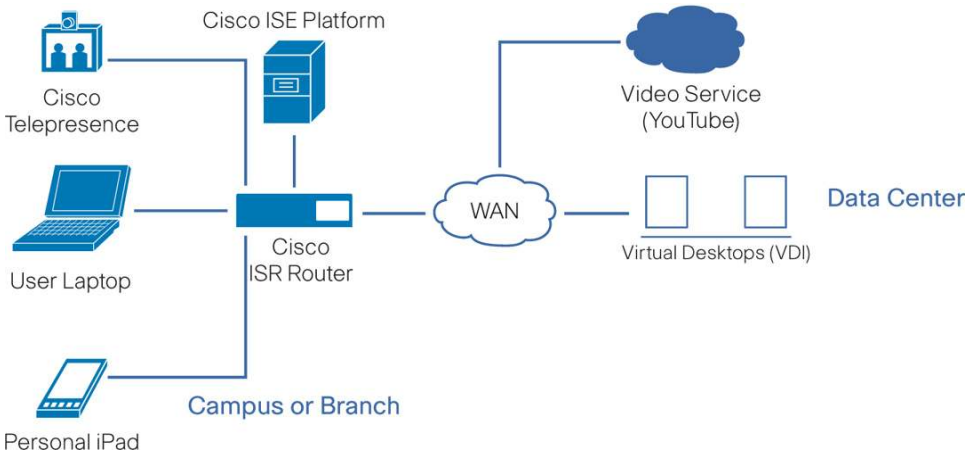


Table 7. Scenario 2: Contextualized Report

User	Device	Location	Resource	Service Context	Action
Tom (role: sales manager)	iPad	San Jose, Building 1	Media traffic	Any	Grant between 9 am to 3 pm
Jim (role: sales manager)	Virtual desktop	San Jose, Building 1	Media traffic	Bronze QoS	Granted, time, duration
John (role: general manager)	Cisco TelePresence	Boxborough, branch office	Customer session	Platinum QoS	Granted, time, duration

Scenario 3:

Ensure that Point of Sale systems and security cameras in a branch location always have high QoS.

Consider a retail environment with multiple branch locations spread out across the country. The branch offices have limited WAN links connecting them to the headquarters site. Top concerns for corporate executives are that

customer transactions always succeed and that the company's security personnel have the ability to conduct surveillance at branch locations using IP-based cameras.

This is a typical scenario for retail networks, where managing multiple configurations across many branches can become time-consuming and potentially prone to errors. Any changes to configurations, such as changing the definition for "after hours," make the network even more complex to administer. How can IT managers enforce different levels of service based on per-device and service context in a scalable, reliable way? A policy solution for this scenario might look as shown in Tables 8 and 9.

Table 8. Scenario 3: Policy Definition

Device	Destination Resource	Service	Action	Condition
Point-of-sale system	PCI servers	Platinum QoS	Set	Corporate-owned
Security cameras	HQ security	Gold QoS	Set	Corporate-owned; after hours period is 6 pm to 6 am

Table 9. Scenario 3: Policy Governed Network, Before and After

Before	After
• Point-of-sale (POS) systems and IP-based surveillance cameras are connected statically to a VLAN. • Network teams define QoS per VLAN to provide appropriate level of service. • Manual intervention or scripting is required to change level of service after hours to comply with policy. This is costly and high-touch, prone to inconsistent behavior due to manual intervention. • Lack of contextualized visibility of what devices are connecting across the branch network. • When new POS devices are added, or when POS devices are mobile, similar configuration is needed in the wired and wireless network devices.	• Business relevant policies are defined in Cisco ISE platform. • Cisco ISE detects and classifies devices as security cameras and POS systems. • Attributes such as location, time, and service accessed are collected. • Network devices such as the branch Cisco ISR router get the policy context and enforce the policy based on device, device context, and service. • Consistent visibility is provided, showing the device, location, and service offered.

The Policy Governed Network would be able to automatically detect and classify the POS equipment and surveillance cameras on the network. Based on real-time awareness, policies can be dynamically enforced through the branch network infrastructure (Figure 6 and Table 10).

Figure 6. Scenario 3: Network Diagram

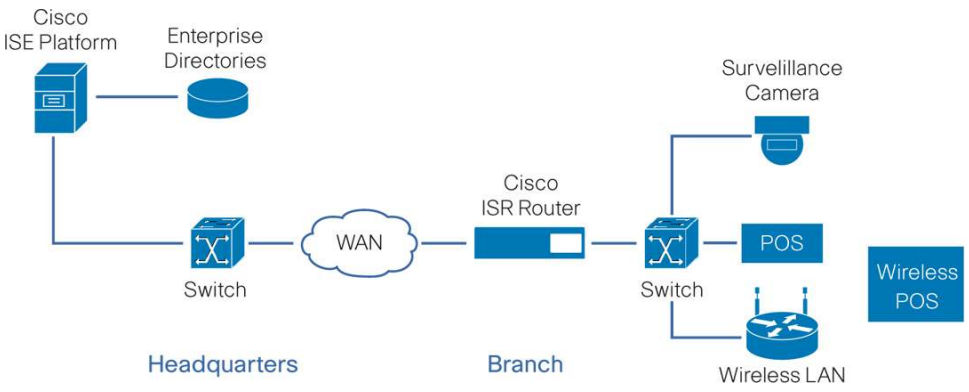


Table 10. Scenario 3: Contextualized Report

Device	Destination Resource	Time	Location	Service Context	Action
POS (company - owned)	PCI server	17:30	San Francisco branch	Platinum QoS	Granted, time
IP camera (company - owned)	Video server at headquarters	18:01	Philadelphia branch	Gold QoS	Granted, time
IP camera (unknown)	External video server	16:05	Las Vegas branch	Any	Denied, alert

How to Begin the Transition

Cisco's Identity Services Engine provides the foundation for the Policy Governed Network architecture with an identity-based policy management system that helps managers to meet IT and business needs in the areas of security and compliance. The Cisco ISE platform secures enterprise networks by building and enforcing identity- and context-based access policies for users and devices, while protecting critical data throughout the network.

Cisco ISE lays the foundation by allowing managers to define and enforce contextual policies based on these facets of identity:

- **Who?** What are the identities and permissions associated with all the authorized users and the devices that need dynamic access to the network? How do you deal with users who wish to use consumer devices such as iPads, smartphones, or Cisco Cius™ tablets in their work? How do you detect network-capable, purpose-built devices anywhere on your network? How do you differentiate rogue devices from legitimate ones?
- **What?** What resources are users and devices trying to access on the network? Are they entitled to access these resources?
- **Where?** In what locations and in what types of networks do you want to enforce policies to protect your assets and intellectual property? Because the borders between networks have blurred, will you need to provide "anywhere" access?
- **When?** At what time of day is the user and device trying to access network resources?
- **How?** In what manner and with what resources do you want to establish, monitor, and enforce consistent global access policies?

By deploying the Cisco ISE platform to enforce secure access policies today, IT organizations will be able to enforce identity-and context-aware policies in additional network domains, including virtualization and branch office service prioritization, in the future.

For More Information

Cisco is committed to helping customers define and implement a Policy Governed Network architecture and deploy the Cisco ISE platform in their infrastructure. To help guide you through an initial Cisco ISE deployment, Cisco recommends that you take advantage of the advisory services available through Cisco Services or our partner community. We invite you to discuss your strategy with your Cisco account manager, channel partners, and other IT advisors.

For additional information on Cisco ISE and related technologies, visit http://www.cisco.com/go/ise.

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 C11-663616-00 07/11