

What Problems Need to be Solved

Many organizations deploy wireless networks to enable flexibility in their computing environments and to more efficiently mobilize their workforce. But this flexibility may result in poor quality of service (QoS) for critical applications, especially latency-sensitive applications such as voice or video. With QoS technology, the network infrastructure delivers a defined level of service to an application so that the application can meet its performance requirements. QoS can distinguish between different traffic types to allocate resources on the network, ensuring that critical applications receive the most efficient use of the network. In the face of network congestion, traffic managed with QoS performs much better than traffic without QoS enabled.

Due to the inherent mobility of users in Wireless networks, it can be difficult to properly allocate appropriate bandwidth to prioritize important applications. Users are free to move from one area to another, dynamically creating network congestion in areas where previously there was none.

The IEEE 802.11e standard addresses some QoS issues related to wireless, such as the downstream performance from the access point to the client. However, 802.11e does not differentiate between node or application types; this leaves latency-sensitive or critical traffic vulnerable to loss or delay on the upstream connection from the client to the access point.

Since 802.11e does not provide QoS on a per-application basis, traffic from critical applications, such as financial or healthcare information, is treated the same as less-critical e-mail or Web browsing traffic. This worsens contention and congestion in the wireless network, delivering poor overall application performance. Wi-Fi Multimedia (WMM) capable devices that support a subset of the 802.11e standard are able to classify traffic types, but these self-appraised markings cannot always

be trusted due to potential misuse from unauthorized applications. The benefits gained from deploying wireless will be minimized or negated if users cannot run important applications because of poor performance.

What Are the Wireless Benefits of Cisco Security Agent?

Cisco Security Agent Wireless Optimization

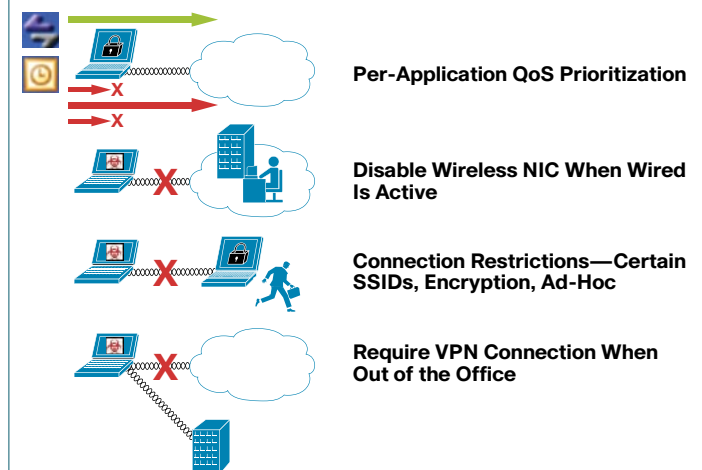
Cisco® Security Agent enhances 802.11e and WMM technology deployments by providing QoS policies on upstream traffic to set and validate Differentiated Services Code Point (DSCP) markings on a per-application basis (for example, marking financial traffic as mission-critical, and Web traffic as best-effort). These DSCP markings are inserted into the IP headers of transmitted packets and used by devices upstream in the wireless network to classify the packets and apply QoS service policies to prioritize that traffic accordingly. Cisco Security Agent allows this to be done at any level on the client: per protocol, per port ranges for a given protocol, and most importantly, per-application per-port per-protocol, which gives administrators a high level of control over which traffic to prioritize. Cisco Security Agent provides QoS to all applications, regardless of whether they were originally built with it. Cisco Security Agent also allows an organization to use any existing legacy, non-WMM devices to provide QoS for critical applications by marking application flows on their behalf.

Cisco Security Agent consists of host-based agents, deployed on desktops and servers that report to the Cisco Management Center for Cisco Security Agents. The Management Center runs as a standalone application performing all management functions in a centralized manner. Its role-based, Web-browser access makes it easy for administrators to centrally create or modify QoS policies across all endpoints.

Wireless Policy Controls

In addition to providing QoS performance for critical applications, any wireless deployment strategy should contain a security policy. Cisco Security Agent provides wireless policy controls to enhance the overall security of the wireless deployment and minimize risky behavior by wireless users. Policies can restrict wireless connections to specific parameters, such as requiring a VPN connection for wireless traffic when a user is out of the office. Cisco Security Agent's location-based policy controls offer an additional layer of protection by providing the capability to restrict access to confidential files or critical applications when a user is remote. Simultaneous use of wireless and wired network interfaces can be prevented, and restrictions can be placed on the usage of ad-hoc mode or specific wireless encryption types, resulting in increased security levels. Wireless broadband cards can be differentiated and their usage restricted as needed based on card type to prevent the use of a personal wireless broadband card with a corporate-owned laptop.

Figure 1. Cisco Security Agent Wireless Control





What Is Cisco Security Agent?

Cisco Security Agent goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because Cisco Security Agent analyzes behavior, its solution provides robust protection with reduced operational costs.

Cisco Security Agent resides between the applications and the kernel, enabling maximum application visibility with minimal impact to the stability and performance of the underlying operating system. The software's unique architecture intercepts all operating system calls to file, network, and registry sources, as well as to dynamic run-time resources such as memory pages, shared library modules, and COM objects. The agent applies unique intelligence to correlate the behaviors of these system calls, based on rules that define inappropriate or unacceptable behavior for a specific application or for all applications. This correlation and subsequent understanding of an application's behavior are what allows the software—as directed by the security staff—to prevent new intrusions.

When an application attempts an operation, Cisco Security Agent checks the operation against the application's security policy, making a real-time allow or deny decision on its continuation and determining if logging the request is appropriate. By combining security policies that implement distributed firewall, operating system lockdown and integrity assurance, malicious mobile code protection, and audit event collection capabilities in default policies for servers and desktops, Cisco Security Agent provides defense-in-depth protection for exposed corporate systems.

Why Cisco Security Agent?

Wireless networks enable a great deal of flexibility and freedom, but also cause organizations to rethink how they secure their networks and devices to prevent attacks and misuse that would expose critical assets and confidential data. Cisco Security Agent is an important part of an organization's overall wireless security policy, to prevent malicious attacks and employee misuse which can compromise data privacy.