

Protecting and Optimizing Higher Education Networks: Cisco Campus Secure

Executive Summary

At today's colleges and universities, the campus network supports a growing number of research, communications, and educational functions. But with thousands of users, endpoints, and applications active at any time, campus networks are becoming increasingly difficult to protect. Academic IT professionals are constantly challenged to ensure that all devices logging onto the network are secure, to effectively identify and mitigate network attacks, and to protect limited bandwidth resources from abuse and misuse. Meanwhile, new generations of viruses, worms, and malicious code continue to evolve and pose new threats to academic services and assets.

In the face of these threats, today's colleges and universities have access to a wide range of powerful network defenses. But most of these solutions were designed to support enterprises and are not always a perfect fit for more open, diverse academic environments. Now, the Cisco Campus Secure program offers a broad portfolio of threat defense, identity management, and bandwidth control solutions that are ideally suited for academic institutions. Together, these solutions provide the pervasive, proactive, and intelligent network defenses that institutions of higher learning need to safeguard and optimize the academic network.

Overview

The campus network now plays an integral role in the core mission of colleges and universities. Network applications such as cluster computing, digital libraries, IP telephony, and IP-based distance learning are increasingly becoming critical services, and they must be delivered with the same degree of reliability as any other utility. But unlike a university's water or electricity system, the IP network is under constant threat of attack: from viruses and worms, from malicious users intent on compromising secured systems, and even from seemingly benign applications such as peer-to-peer (P2P) file sharing, which sap limited bandwidth resources from critical academic services.

These threats can have serious consequences. An infection originating in just a single computer (which may not have been properly used or updated) can propagate a worm or virus through the entire campus network within minutes. If such network attacks do not destroy or steal data, they often cause storms of excess traffic and seriously impair an institution's ability to function, resulting in downtime and lost classroom time.

Colleges and universities have deployed a variety of network defenses, but with newer, faster-propagating attacks appearing all the time, even the best defenses have trouble keeping pace. Education networks typically include hundreds of devices and support thousands of users, resulting in thousands of active IP flows. Simply distinguishing a true network attack from benign behavior—much less responding to an attack, once identified—is extremely difficult. Enforcing uniform security policies across a diverse academic user base while trying to preserve the inherent openness of the academic environment is also a challenge. And, as for provisioning and controlling bandwidth resources across thousands of users, groups, and applications, colleges and universities have historically found few effective tools.

Today's colleges and universities are beset by:

- **Environmental challenges**—IT administrators struggle to ensure the security and availability of critical network applications while maintaining the open, unfettered learning environment that academic institutions require.
- **Expanding user base**—At a typical college or university, thousands of unique endpoints connect to the network every day. Administrators need new tools to distinguish between secure and unsecure endpoints, and to promote responsible behavior among users.
- **Bandwidth issues**—The rise of bandwidth-intensive P2P traffic and gaming applications demands more effective bandwidth control tools. According to an article in the Chronicle of Higher Education, one university found that 10 students using file-sharing applications for music and movies were consuming 50 percent of campus bandwidth.

- **Evolving network attacks**—The tools to create and propagate network attacks have become more sophisticated, and are increasingly accessible to malicious parties on and off campus. Propagation times are also decreasing, as is the available time to respond to an attack before it causes widespread damage. A recent survey conducted by the Chronicle of Higher Education and Gartner, Inc. revealed that nearly all respondents had experienced virus and worm attacks in the past year; 73 percent said that those attacks are accelerating.
- **Substantial potential costs**—If a network security breach results in the compromise of thousands of user records, the notification effort alone can be a massive and costly undertaking. Stricter government regulations and privacy mandates also increase an institution's legal exposure. Most important, a serious security breach can compromise productivity for students and faculty, and tarnish an institution's reputation.

Most critically, if the campus network relies on individually deployed security solutions that are not integrated into an institutionwide system, responding to any of these needs is a difficult, complex, and costly proposition.

Cisco Campus Secure for Higher Education Networks

Faced with these issues, many colleges and universities are searching for more intelligent, proactive strategies for protecting and optimizing academic networks. Cisco Campus Secure for Higher Education Networks provides a suite of powerful solutions. Designed to support complex, open academic environments, these solutions allow colleges and universities to gain unprecedented insight into network activity, more tightly control network resources and bandwidth resources, and more effectively identify and respond to security threats.

Cisco Campus Secure for Higher Education Networks comprises three core solutions:

- **Cisco Identity Management and Network Admission Control for Education Networks**—This helps ensure that users and devices attempting to gain access to the network are secure.
- **Cisco Self Defending Network for Education Networks**—This includes core, edge, and host security technologies, as well as next-generation solutions that allow administrators to more effectively identify and mitigate network attacks.
- **Cisco Bandwidth Control for Education Networks**—This provides intelligent tools for controlling and protecting bandwidth resources.

Individually, these solutions and their constituent components offer a variety of tools to create a more secure and better-performing academic network. When combined as part of an integrated Cisco Campus Secure strategy, they provide an extremely powerful, versatile, and comprehensive platform for protecting and optimizing campus networks.

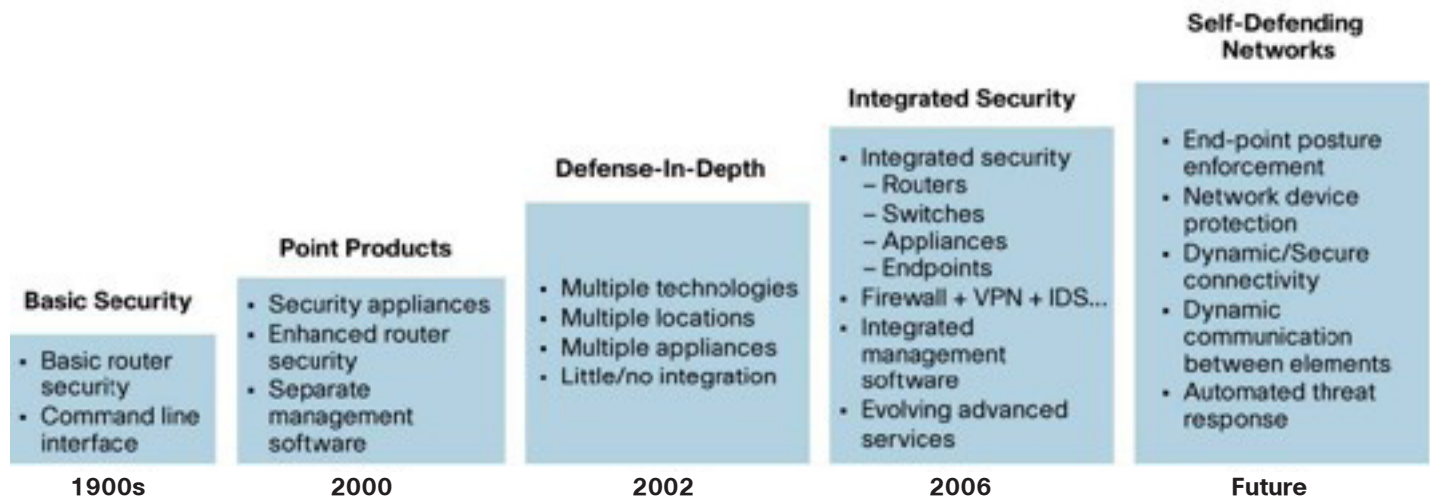
The Self-Defending Network

Cisco Campus Secure for Higher Education Networks is based on the Cisco Systems vision of the Self-Defending Network—a network that is integrated, collaborative, and adaptive. A Self-Defending Network:

- Integrates security throughout all aspects of the network
- Collaborates among all network and security elements to create a unified defense system
- Adapts to new threats as they arise

All the solutions within Cisco Campus Secure for Higher Education Networks are designed to help colleges and universities achieve these goals. All draw on the embedded intelligence of Cisco routers and Cisco Catalyst switches deployed in the network, and incorporate multiple Cisco infrastructure components and security components into a single network security framework. These solutions promote a more intelligent, responsive academic network that can constantly evolve to respond to new challenges. As a result, colleges and universities that embrace the Cisco Campus Secure for Higher Education Networks strategy can implement a more pervasive, effective network defense system, while maximizing the existing network and security infrastructure investment (Figure 1).

Figure 1. Higher Education Network Security Evolves from Point Products to an Integrated, Self-Defending Network



Cisco Identity Management and Network Admission Control For Higher Education

The first step in protecting university networks is controlling who and what can gain access. As many colleges and universities learned in the wake of recent worm attacks, once students begin connecting to the network with infected PCs, an attack can rapidly disable critical services and wreak havoc across the campus network. But while many colleges and universities are keenly aware of the problem, it is extremely difficult to mitigate this threat. After all, the nature of campus life means that thousands of users—many with their own unique PCs, antivirus systems, and operating system vulnerabilities—will regularly connect to the campus network.

In the past, colleges and universities have tried a variety of strategies to enforce uniform access control policies, including requiring users to install antivirus software and operating system updates, and requiring students to register and authenticate their PCs. But these strategies could not provide robust protection. It's easy to announce policies about antivirus software and operating system updates but much more difficult to enforce them. And user registration establishes the presence of an authorized user, but does nothing to ensure that the user's PC meets the security policies of the institution.

Over the past several years, a new strategy has emerged that provides the intelligent, proactive mechanisms for user authentication and access control that academic networks require: Network Admission Control (NAC). NAC allows universities to automatically detect, isolate, and clean infected and/or vulnerable wired and wireless devices that attempt to access the campus network. Developed by Cisco, NAC brings together leading solutions in antivirus systems, network security, and network management to ensure that all devices in the network comply with university security policies, and to repair any vulnerabilities (such as out-of-date antivirus or operating system software) before permitting access to the network.

As a core component of Cisco Campus Secure for Higher Education Networks, Cisco Identity Management and Network Admission Control offers colleges and universities a choice of two NAC solutions to provide this critical service (Figure 2). Both solutions extend uniform trust and identity policies throughout the campus network, including the wired infrastructure, wireless LANs and devices, and remote access VPNs.

Universities can choose from appliance-and architecture-based approaches to NAC:

- [Cisco NAC Appliance](#)—Provides appliance-based NAC services, and can operate within any network environment
- [Cisco Network Admission Control \(NAC\) Framework](#)—Provides comprehensive, architecture-based NAC services in Cisco networks that employ 802.1X authentication

Cisco also offers an additional level of protection through the Cisco Identity-Based Networking Services (IBNS) solution. Based on 802.1X port and machine authentication, the Cisco IBNS framework combines solutions for authentication, access control, and policy enforcement to provide a more flexible, effective means of enforcing connectivity and security policies.

Cisco NAC Appliance

Cisco NAC Appliance is a self-contained, appliance-based NAC solution. It combines roles-based authentication, vulnerability assessment, policy enforcement, and distributed remediation into a single, easy-to-deploy solution. The Cisco NAC Appliance consists of:

- **Cisco Clean Access Servers**—which evaluate endpoints attempting to gain access and enforces access privileges based on compliance with the institution's security policies
- **Cisco Clean Access Manager**—a centralized, Web-based console for establishing roles, checks, rules, and policies
- **Cisco Clean Access Agent**—an optional thin client that can be deployed on user devices to enhance some vulnerability assessment functions and streamline remediation processes

Together, these components allow the Cisco NAC Appliance to provide:

- **Authentication**—Cisco Clean Access servers integrate with the authentication servers and mechanisms already in use within the network and enforce security policies for all devices attempting to gain access.
- **Vulnerability assessment**—The Cisco NAC Appliance can scan all Windows-based operating systems, Mac OS, Linux machines, and even non-PC networked devices—such as gaming systems and personal digital assistants (PDAs)—for viruses, malicious code, and other security vulnerabilities.
- **Remediation and repair**—When a noncompliant device is detected, the solution can place it into quarantine, preventing the spread of a virus while allowing the device to access remediation resources, such as operating system patches and virus definition files.
- **Centralized management**—The entire Cisco NAC Appliance—including all servers and endpoint agents—can be managed with a single, Web-based management console. Administrators can define and update security policies, and set policies for different types of devices, users, and roles.

Benefits of the Cisco NAC Appliance

With the Cisco NAC Appliance colleges and universities can enforce institutional security policies more effectively than ever before and can better protect the campus network. As an appliance-based NAC system, Cisco NAC Appliance offers a streamlined, easy-to-implement solution for deploying critical NAC functions in university networks that cannot support an architecture-based NAC strategy.

The Cisco NAC Appliance solution allows colleges and universities to:

- Reduce network outages caused by viruses and worms
- Improve compliance with security policies by making compliance a fundamental requirement for access to the network
- Minimize vulnerabilities on user machines through periodic evaluation and remediation
- Realize significant cost savings by automating the process of repairing and updating user machines

Cisco Network Admissions Control Framework

Cisco NAC Framework provides a pervasive, architecture-based NAC solution, in which trust and identity systems are embedded in the network infrastructure itself. Developed through an industrywide collaboration led by Cisco Systems, the Cisco NAC Framework is designed to closely interoperate with Cisco network technologies and partner security and management solutions in sophisticated network environments. These NAC services incorporate the 802.1X authentication protocol and 802.1X functionality of the switches, routers, wireless access points, and security solutions already deployed in the network. (Under the updated NAC Framework, NAC version 2, the full range of Cisco routers, Cisco Catalyst Layer 2 switches and Layer 3 LAN switches, and Cisco Aironet wireless access points support NAC functionality.)

These infrastructure devices communicate with software agents deployed on user endpoints to enforce security policies and dynamically quarantine and/or remediate infected devices attempting to access the network. As a result, colleges and universities can handle comprehensive endpoint security and management with their existing access control systems and security policy systems—without requiring any additional network devices to perform these functions.

Cisco NAC Framework incorporates:

- **Communication agents**—Cisco Trust Agent software collects security state information (such as whether antivirus software and operating systems are up to date) from the endpoint and communicates this information to the network access device.
- **Network access devices**—Every device seeking network access initially contacts a network access device, such as a router, switch, firewall, or VPN concentrator. These devices demand security “credentials” from the endpoint and relay that information back to the central policy servers for an admission decision.
- **Policy servers**—The institution’s Cisco Secure Access Control Servers (ACS) or third-party policy servers evaluate the endpoint security credentials and determine whether to permit, deny, quarantine, or restrict access.
- **Management systems**—Network security management consoles that support NAC, such as the CiscoWorks VPN/Security Management Solution (VMS) and CiscoWorks Security Information Manager Solution, provision some NAC elements and provide monitoring, reporting, and management of endpoint security applications.

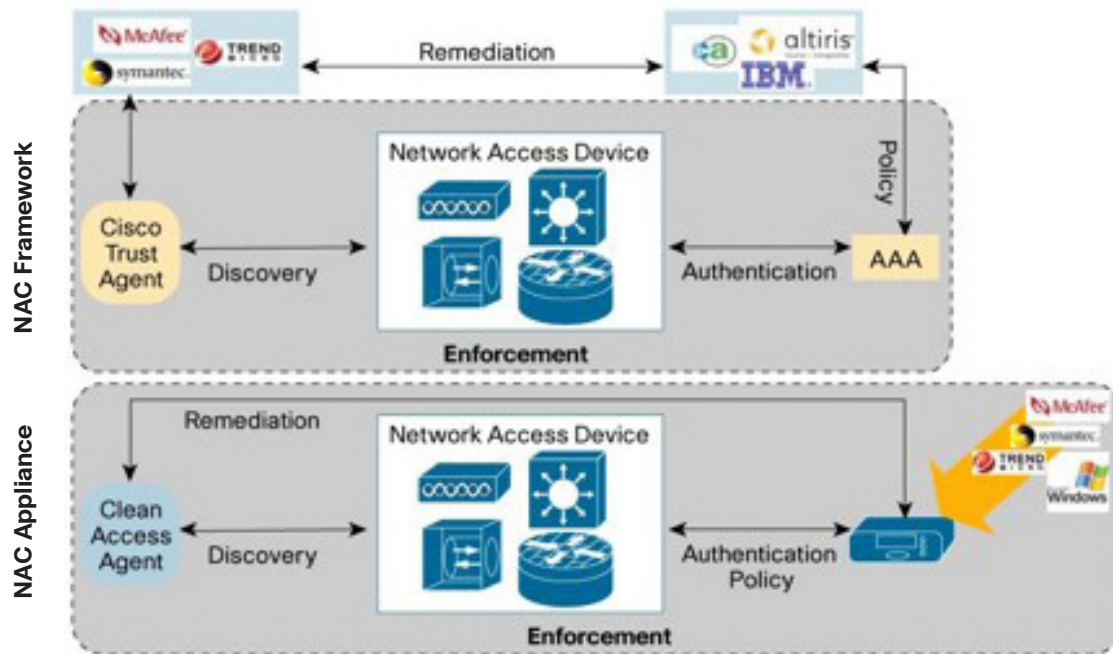
Benefits of Cisco NAC Framework

By integrating NAC services with the network architecture itself, universities gain:

- Dramatically improved security through comprehensive control of all endpoints across all access methods, including LAN, WAN, wireless, and remote access
- Endpoint visibility to help ensure that managed, unmanaged, guest, and even rogue devices comply with university security policies
- Extended benefits from deployed network infrastructure and antivirus systems, since the NAC Framework integrates and enhances the functionality of these systems
- Lifecycle support that automates the assessment, authentication, authorization, and remediation of endpoints
- Granular admission control management delivered by a combination of centralized policy management and intelligent network devices and services, incorporating solutions from many leading antivirus, security, and management vendors
- A standards-based approach to NAC that allows for easy integration with partner solutions and security services

Figure 2. Comparison of the Cisco NAC Appliance and the Cisco NAC Framework

NAC Framework: Vendor products provide assess and remediate an intelligent network Cisco NAC Appliance: Turnkey NAC appliance for authentication, assessment, and remediation



Cisco Identity-Based Networking Services

Distinguishing trusted users from untrusted users in open academic networks is always challenging. Colleges and universities need mechanisms that allow individual users to access certain resources (such as the Internet) while being denied access to others, such as internal university servers.

The Cisco Identity-Based Networking Services (IBNS) solution provides this capability by combining authentication, access control, and user policies into a single framework. With the Cisco IBNS solution, colleges and universities can set access policies for individual users and sets of users (instead of setting policies for physical ports), and implement much more granular, flexible processes for connectivity and policy enforcement.

At the heart of the Cisco IBNS solution is the access control features of the 802.1X authentication protocol, supported by the full range of Cisco routers, Cisco Catalyst switches, and Cisco Aironet wireless access points. These features provide secure internal resources with an extra layer of protection by requiring all devices attempting access to them to present valid access credentials. Since the system is integrated with the institution's central authentication and policy enforcement systems, colleges and universities also gain extraordinary flexibility to set access policies on a per-port, per-user, or per-group basis.

Benefits of the Cisco IBNS Solution

With the Cisco IBNS solution and its 802.1X capabilities, colleges and universities can:

- More easily authenticate, authorize, and account for all users of wired and wireless networks through flexible user profiles and group profiles that define trust relationships
- Provide users with more mobility and freedom, since access and security policies are associated with users, not physical ports
- Enhance scalability and ease of management of policy enforcement and provisioning
- Block rogue wireless access points from gaining access to secure network resources by requiring appropriate credentials from all devices requesting access

Cisco Self Defending Network for Education Networks

Trust and identity management systems are a critical first step in academic network defenses, but they do not ensure complete protection. So colleges and universities have deployed a variety of core security solutions (such as firewalls, intrusion detection and intrusion prevention services, and host-based security mechanisms) to provide multiple layers of defense against network threats. But if the network relies on individually deployed security solutions that are not integrated into an institutionwide system, it is a complex proposition to accurately identify, correlate, visualize, prioritize, and mitigate attacks in progress.

Cisco Self Defending Network for Education Networks provides a suite of tools and services that tightly collaborate with the embedded security capabilities in Cisco network devices, and delivers the intelligence and functionality that academic network defenses require. The solution focuses on two critical areas of network security: timely identification and mitigation of security threats, and integration of security services into the network architecture itself.

This strategy incorporates:

- **Core security solutions**—Which include firewalls, IDS/IPS sensors, endpoint security mechanisms, Layer 2 and Layer 3 Security services, content security, and security management systems, working together to create a robust foundation for protecting academic networks
- **Cisco Security, Monitoring, Analysis, and Response System (Cisco Security MARS) appliances**—Which provide comprehensive security monitoring and threat mitigation
- **Cisco ASA 5500 Series Adaptive Security Appliances**—Which reduce the complexity of managing multiple standalone security solutions by combining firewall, intrusion prevention, application security, network antivirus, and VPN technology into a single device

The Self-Defending Network strategy at the heart of the Cisco Campus Secure program relies on a variety of network infrastructure and security devices communicating and collaborating to create a unified defense. These components include:

- **Firewalls**—Stateful firewall solutions such as Cisco PIX™ Security Appliances defend the network perimeter by filtering hosts and services, inspecting incoming traffic at a granular level, limiting inbound connections, and blocking access to protected internal resources.
- **Intrusion detection services (IDS) and intrusion prevention services (IPS)**—IDS and IPS provide an additional layer of protection by policing traffic across the network, detecting potential threats, and sometimes blocking ports to prevent malicious behavior. These services can be delivered via IDS/IPS sensor appliances or by the network itself, through solutions such as the Cisco Network-Based Intrusion Detection System (NIDS) and the IPS/IDS features embedded within the Cisco IOS™ Software in Cisco network devices.
- **Endpoint security**—Endpoint security agents, such as Cisco Security Agent, go a step beyond antivirus solutions by detecting any suspicious operating system behavior—as opposed to detecting known virus signatures—and can protect user endpoints against both known and unknown (or “day zero”) attacks. Cisco Security Agent integrates with Cisco NAC Framework to provide more granular security state information about an endpoint requesting access, but also continues to protect that endpoint when it is not connected to the academic network.
- **VPN connectivity**—Virtual private networks have become the most popular mechanism for providing secure remote connectivity due to their low cost, robust encryption, and simple deployment and management. Colleges and universities can deploy VPN appliances such as Cisco VPN 3000 Series Concentrators, or use the embedded VPN capabilities in Cisco routers and Cisco Catalyst switches.
- **Layer 3 security services**—Cisco IOS Software Advanced Security Features in Cisco routers deployed in the network can provide enhanced Layer 3 security services. With these features, academic IT administrators can automate router security configurations, identify and prioritize different types of traffic (such as file-sharing applications), limit bandwidth or memory usage on specific network segments, and provide NetFlow information to network management systems.
- **Switch-based security services**—Cisco Catalyst switches offer enhanced Layer 2 and Layer 3 security services to help colleges and universities better control traffic across the campus network. Cisco Catalyst switches provide enhanced VLAN capabilities and protect against snooping and port scanning, and can prevent worm or virus infections from flooding ports.

- **Security management**—Sophisticated network security management systems, such as CiscoWorks VMS, provide a variety of tools to more efficiently and cost-effectively configure, monitor, and troubleshoot campus network security systems.

Cisco Security MARS

A large university network may register millions of potential security events every day. Distinguishing false alarms from genuine threats that demand immediate attention can be a monumental task. Many colleges and universities have deployed Security Information Management (SIM) systems in an attempt to better manage this mountain of data. But even these systems generally provide huge, cumbersome reports.

Cisco Security MARS goes beyond conventional SIM systems to efficiently aggregate and synthesize the massive amounts of network and security data typically generated in an education network. The solution uses sophisticated event correlation and validation to help IT administrators appropriately identify and respond to threats. Designed specifically for academic IT environments that have few resources to devote to dedicated network security staff, Cisco Security MARS allows even administrators who are not security specialists to easily identify and respond to attacks.

Cisco Security MARS:

- Automatically discovers the topology of the network and uses this awareness to scan network devices for anomalous behavior and protect against day-zero attacks
- Tightly integrates and collaborates with security services embedded within Cisco network routers and Cisco Catalyst switches to closely monitor network behavior
- Winnows down potential problems to a manageable number of incidents that analysts can further investigate (while preserving details of every potential event in its database for later analysis or reporting purposes)
- Uses intuitive, drill-down topology maps to help administrators better visualize and respond to security events
- Provides tools to prevent, contain, or stop an attack in real time
- Adapts to an evolving environment by applying false positive information to reduce the number of incidents reported in the future
- Supports rule creation, threat notification, and incident investigation processes, as well as a variety of security posture and trend reports, tailored specifically for education networks
- Allows administrators to classify false positives from a single, centralized platform, eliminating the need to fine-tune individual appliances and services throughout the network
- Supports data collection and analysis from Cisco devices and non-Cisco devices alike, providing more comprehensive monitoring

Cisco Security MARS appliances are available in four sizes, depending on the security event processing power an institution requires (Figure 3). The solutions can function individually or in a distributed mode, through the use of a global controller.

Figure 3. Cisco Security MARS Options

	CS-MARS 20	CS-MARS 50	CS-MARS 100	CS-MARS 200		
CS-MARS Model	20	50	100e	100	200	Global Controller
Events/Sec	500	1,000	3,000	5,000	10,000	N/A
NetFlow Flows/Sec	15,000	25,000	75,000	150,000	300,000	N/A
RAID Storage	120GB	120GB	750GB	750GB	1TB	1TB
Rack Size	1 RU	1 RU	3 RU	3 RU	4 RU	4 RU

Benefits of Cisco Security MARS

Cisco Security MARS provides:

- More timely attack mitigation through integrated security intelligence that can recognize threats and recommend action before they can take down an entire network
- End-to-end network awareness, with the ability to identify attackers, targets, and hotspots across all types of network devices and configurations, and present this information graphically to allow quick action
- Streamlined threat identification and response, due to the solution's deep awareness of network topology and addressing schemes, and its ability to reduce millions of security events into a manageable number of actual network incidents
- Increased IT staff efficiency and productivity, since the solution determines whether a security event is a genuine attack or a false positive, thereby dramatically reducing the number alarms to which IT staff must respond
- More comprehensive network protection, due to the solution's sophisticated, patent-pending event correlation engine and robust reporting and analysis capabilities

Cisco ASA 5500 Series Adaptive Security Appliances

In an academic environment, networks constantly face new, highly sophisticated security attacks, as well as embedded data and stealth probing. To better protect the educational environment (and comply with government-mandated information security regulations), colleges and universities have deployed a variety of network security technologies. As described above, these solutions included firewalls, VPN appliances, antivirus systems, Web and application security systems, IDS and IPS appliances, authentication systems, and host-based security mechanisms.




Maintaining multiple layers of defense is critical in a large academic network, but relying on standalone solutions for each of these services (often from multiple vendors) carries a cost: increased network complexity and, often, substantial human and financial management resources. As a result, many colleges and universities are now turning to converged, next-generation network security solutions that can deliver all of these services from a single, integrated platform.

The Cisco ASA 5500 Series combines world-class firewall features, IP Security (IPSec) and Secure Socket Layer (SSL) VPN capabilities, and industry-leading IPS services with a centrally managed, user-friendly GUI. The result is easier setup of security solutions and lower network security management costs.

However, integrating multiple security functions into a single device can also provide better protection. Emerging viruses and malicious code are designed to adapt to a network environment and to develop new strategies for attacking secured assets when their initial attempts fail. In networks that manage all network defense services through separate devices, a threat can get deeper into the network, until it reaches the specific security device capable of stopping it. (For example, a threat that gets past a firewall can continue traveling into the network—infecting multiple systems along the way—until it reaches another IPS device capable of stopping it.) Since the Cisco ASA 5500 Series consolidates several security functions into a single chassis, threats can be stopped at the single point in the network where the solution is deployed.

Like Cisco Security MARS, Cisco ASA 5500 Series appliances are available in several sizes, depending on the performance required (Figure 4).

Figure 4. Cisco ASA 5500 Series Options

	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540
			
School Location	Department	Campus Edge	Campus Core
Performance			
Max Firewall	300 Mbps	450 Mbps	650 Mbps
Max Threat Mitig. (FW+IPS)	150 Mbps	375 Mbps	450 Mbps
Max IPSec VPN	170 Mbps	225 Mbps	325 Mbps
Base Platform Services	Application firewall, IPSec and SSL VPN, and more A/S HA (Upg.) 3 FE t 5 FE	Same as 5510, plus A/A Failover, VPN Clustering, 4 GE + 1 FE	Same as 5520, with higher performance and scalability

Benefits of Cisco ASA 5500 Series Adaptive Security Appliances

With Cisco ASA 5500 Series Adaptive Security Appliances, colleges and universities can:

- Reduce network complexity and network security operational costs by streamlining the management and provisioning of network security services
- More rapidly detect and mitigate security threats, since a converged network security platform delivers all component services with no performance degradation and can stop worms, viruses, and malicious code at line speed
- More easily apply uniform security policies by maintaining a single, comprehensive security services profile
- Activate new security services as needed, without having to deploy new equipment
- Enhance academic network defenses with state-of-the-art, field-proven network security technologies
- Maintain long-term investment protection through an extensive services roadmap that will ultimately incorporate Anti-X, control and containment, and application security services

Most critically, when a single device integrates multiple security services, those services are capable of mutual awareness and communication, providing IT and network security administrators with an extremely powerful tool for protecting education networks. When such a device is combined with an overarching security mitigation system such as Cisco Security MARS, colleges and universities can achieve an even more effective and efficient security environment, and, ultimately, a true Self-Defending Network.

A Comprehensive Approach to Network Threat Defense

Cisco Security MARS and Cisco ASA 5500 Series Adaptive Security Appliance solutions can each offer substantial advantages when deployed individually. Operating together, the solutions provide an even more intelligent, comprehensive, and effective security strategy for colleges and universities.

By combining the industry-leading threat identification and mitigation capabilities of Cisco Security MARS with the integrated security services of Cisco ASA 5500 Series solutions, academic institutions can immediately deliver virtually any security function to any part of the network. And all these services can be managed easily and centrally—even by network administrators who are not dedicated security specialists. Ultimately, colleges and universities can better protect their networks, assets, and users from even the most malicious security threats.

Cisco Bandwidth Control for Education Networks

At many colleges and universities, network bandwidth upgrades to gigabit and 10 gigabit rates support a new class of rich media applications that aid and enhance the educational process. However, with the benefits of increased bandwidth come potential problems: P2P and gaming applications can consume network resources at an even faster rate, sapping bandwidth from educational services. Many emerging DoS and worm attacks are also now designed specifically for bandwidth-rich environments, and can propagate faster than ever before. And representatives of the music and movie industries, in an attempt to track down major violators of copyright laws, are contacting colleges and universities, which could present those institutions with potential liability issues in the future.

Faced with these issues, many colleges and universities are searching for new ways to control, protect, and optimize campus network resources. The Cisco Bandwidth Control for Education Networks solution provides colleges and universities with a powerful set of tools to implement and enforce an institutionwide bandwidth control policy.

The Cisco Bandwidth Control solution comprises four key components:

- **Cisco Service Control Engine**—Provides granular control of high-value Internet service provider (ISP) network connections
- **Cisco IOS Software Bandwidth Control Features**—Implement rate-limiting mechanisms via Cisco Catalyst switches deployed at the core, edge, and distribution layers of the campus network
- **CiscoWorks QoS Policy Manager (QPM) 3.2**—Provides centralized, scalable quality of service policy control and analysis mechanisms
- **Cisco Application and Content Networking System (ACNS)**—Optimizes the delivery of rich media content in bandwidth-constrained networks

Together, these solutions bring superior granularity, flexibility, and control to campus bandwidth policies, and allow for a higher-performance, better-protected network environment.

The Cisco Service Control Engine

The growing popularity of P2P applications creates serious concerns for colleges and universities, causing substantial network congestion and capacity problems, while also raising legal issues about the proper use of copyrighted materials. Internet service providers estimate that downloads of music, games, video, and other content now consume 70 percent or more of broadband bandwidth. And P2P traffic will only increase as Web-based gaming and video applications mature.

P2P traffic is also difficult to detect: Sophisticated P2P protocols can dynamically hop to different ports, making them difficult to monitor and control. In addition, the high-speed connection from a college or university to its ISP is the most heavily used link in the academic network. Controlling the use of that link is critical, but doing so requires a sophisticated combination of hardware and software capable of packet-by-packet inspection at line rate.

The Cisco Service Control Engine (SCE) provides the extraordinary visibility into network users and applications that academic institutions require, allowing academic IT administrators to more effectively manage P2P traffic and protect ISP links. The Cisco SCE solution provides:

- Aggregated rate limiting, which allows administrators to restrict P2P traffic to a certain percentage of the available bandwidth and reduce the impact this traffic can have on other network services
- Upstream control limits to control P2P file uploads that consume excessive bandwidth, while allowing downstream traffic—and approved upstream traffic—to continue uninterrupted
- Destination-based classification to limit traffic that uses expensive or particularly congested links, peering points, or transit connections
- Time-of-day policies that enforce different limits on P2P usage at different times, effectively encouraging P2P application users to shift their activities to hours when P2P traffic will have the least impact on the network and other users

- User application quotas that enforce a byte cap, such as a per-day quota, on P2P applications, after which access to these applications can be blocked or throttled to a minimum, while other critical academic applications remain fully available
- User dynamic policies that allow institutions to create subscription packages or “bandwidth-on-demand” services, through which users can control their own accounts and pay for additional bandwidth if they choose to use P2P services

Cisco IOS Software Bandwidth Control Features

As a complement to the Cisco Service Control Engine, many Cisco Catalyst Series switches can incorporate rate-limiting mechanisms to police and restrict traffic flows. These capabilities provide an extraordinary degree of flexibility in bandwidth control, allowing colleges and universities to allocate bandwidth on a per-user, per-group, or per-application basis. With strict policies enforced at the core, edge, and distribution layers of the network, users can send and receive only up to the bandwidth individually allocated to them. Institutions can even single out certain groups (such as faculty or research students) or devices (such as application servers) for additional bandwidth, while providing baseline performance for all users.

Cisco switching solutions with available Cisco IOS Software bandwidth control features include:

- [Cisco Catalyst 6500 Series and 4500 Series switches](#)—The Cisco Catalyst 6500 Series Supervisor 720 module and the Cisco Catalyst 4500 Series Supervisor V-10GE module provide user-based rate limiting (UBRL) capabilities to identify and enforce limits on unique traffic flows. The solutions can support tens of thousands of individual flows and hundreds of different rates, and they allow institutions to enforce strict bandwidth policies from the network core to the distribution layer, on a per-user or per-group basis. Institutions can also implement separate rate-limiting strategies for dormitories or other campus buildings, based on the likely usage patterns of users.
- [Cisco Catalyst 3750 Series switches](#)—This family of switches supports an extensive rate-limiting feature set that can be applied on both Gigabit Ethernet and Fast Ethernet interfaces. Education IT managers can set policies to allocate higher or lower bandwidth to certain users, groups of users, or applications. Institutions can even single out certain groups (such as faculty or research students) or devices (such as application servers) for additional bandwidth, while providing baseline performance for all users.

Assigning Scavenger Class Traffic

One Cisco IOS Software bandwidth control feature provides colleges and universities with the ability to apply a “scavenger class” policy to recreational gaming and P2P traffic. The scavenger class, based on an Internet II draft, is intended to provide deferential services, or “less-than-besteffort” services, to certain applications. Applications assigned to this class—including P2P media-sharing applications (such as KaZaa, Morpheus, and Grokster), gaming applications, and any entertainment video applications—have little or no contribution to the institutional objectives of the education network. By assigning a minimal bandwidth queue to scavenger traffic, universities can limit this traffic to virtually nothing during periods of congestion, but allow it to be available if bandwidth is not being used for educational purposes. This way, institutions can apply more flexible, nonstringent policy control to noneducational applications.

Scavenger-class functionality can also play a significant role in mitigating DoS attacks and worms. When campus security systems identify uncharacteristic spikes in network activity (which usually suggest a DoS or worm attack), scavenger-class capabilities allow the systems to dynamically reassign that traffic to a much lower class of bandwidth, limiting the attack’s ability to rapidly propagate itself.

CiscoWorks QoS Policy Manager 3.2

Even the most sophisticated bandwidth control mechanisms are useless if they cannot be easily implemented and managed in a scalable way. As part of the CiscoWorks network management solution, CiscoWorks QPM 3.2 is a secure, Web-based tool that provides end-to-end quality of service for converged data, voice, and video networks. CiscoWorks QPM 3.2 provides the ability to monitor and prioritize traffic across the IP infrastructure by taking advantage of the QoS mechanisms embedded within Cisco switching and routing equipment. As a result, institutions can more easily scale bandwidth control services across the network and enforce institutionwide bandwidth control policies.

CiscoWorks QPM 3.2 allows campus IT administrators to gain greater visibility into network traffic flows, which helps enable them to configure appropriate policies for campus applications, and automate the provisioning of multiple service levels across the campus network. After QoS is deployed, CiscoWorks QPM 3.2 also provides detailed information about traffic patterns, which allows campus IT staff to determine if the QoS policies are having the desired impact. Network administrators can view QoS graphs next to policy descriptions and troubleshoot performance problems by examining traffic patterns relative to QoS enforcement mechanisms. Administrators can even use a date and time “zoom” function to scan QoS data over different time periods, and a file export function to perform analysis with other tools.

Cisco Application and Content Networking System

In some regions of the world, because of the cost of high-speed WAN links, colleges and universities must rely on T1, E1, or even smaller circuits to support the academic network. In these environments, institutions can have a difficult time delivering rich media content and innovative educational applications. The Cisco ACNS solution optimizes content delivery in bandwidth-constrained networks, reducing network congestion by storing and delivering content at the network edge.

Cisco ACNS Software combines the technologies of demand-pull caching and pre-positioning of Web applications, objects, files, and streaming media to accelerate content delivery. The solution runs on Cisco Wide-Area Application Engine (WAE) appliances, Cisco Content Distribution Manager (CDM), and Cisco Content Router platforms.

Together, these intelligent hardware and software components provide:

- Reduced WAN congestion by storing and delivering content at the network edge through the use of the Cisco WAE appliance or Cisco WAE Network Module
- Centralized content management capabilities through the use of the Cisco CDM appliance and through the sophisticated network and device management tools in the CiscoWorks software suite
- Content routing capabilities, including the HTTP routing features of the Cisco Content Router appliance and the Web Cache Communication Protocol (WCCP) functionality embedded in Cisco routers and switches

Benefits of Cisco Bandwidth Control

Together, the technologies in the Cisco Bandwidth Control for Education Networks solution provide a comprehensive strategy for more effectively controlling campus bandwidth and enforcing institutionwide bandwidth control policies.

Cisco Bandwidth Control for Education Networks provides:

- Effective bandwidth control in each functional area of the network—By managing heavily used ISP links with the Cisco Service Control Engine, by managing bandwidth in the network core, distribution, and edge layers with the rate-limiting capabilities of Cisco IOS Software, and by allowing institutions to easily scale uniform bandwidth control policies across the campus network with CiscoWorks QPM 3.2
- Reduced costs—By eliminating the need to upgrade network infrastructure prematurely to accommodate growing P2P and gaming applications, while reducing P2P application usage of more expensive network links and peering points
- Reduced network congestion—By tightly controlling P2P traffic and pre-positioning rich media content at the edge of bandwidth-constrained networks
- Enhanced protection against DoS and worm attacks—By allowing academic IT administrators to throttle down bandwidth allocated to any user or application, limiting the damage of security attacks designed to exploit high-bandwidth environments
- Improved network and application performance—By restricting nonessential P2P and gaming traffic, while helping to ensure that critical applications and groups always have the network resources they need

Cisco Lifecycle Security Services

The network defense strategies in Cisco Campus Secure for Higher Education Networks can dramatically improve academic network defenses, but technologies alone are not enough. To keep pace with a constantly changing environment and rapidly evolving threats, colleges and universities also need ongoing support and services.

Cisco Systems and its partners provide a broad portfolio of end-to-end services and support that can help colleges and universities reduce network total cost of ownership, increase network availability, and enhance the value of the academic network.

The Cisco Lifecycle Services approach defines the minimum set of activities needed, by technology and by network complexity, to help institutions successfully deploy and operate Cisco technologies and optimize the performance of those technologies throughout the network lifecycle. This approach can help academic institutions achieve a high-performance network, integrate advanced technologies, lower operational costs, and maintain network health and security through day-to-day operations.

Cisco security services span the Prepare, Plan, Design, Implement, Operate, and Optimize phases of the network lifecycle, and include:

Prepare

[Cisco consulting services](#)—Provide the security vision for the future and help ensure that institutional goals incorporate security planning

Plan

- [Security Posture Assessment Services](#)—Assess the network's current state of security
- [Incident Readiness Services](#)—Evaluate how effectively current security processes and technologies respond to an attack
- [IP Communications Security Review Services](#)—Promote appropriate protection for voice communications in converged voice and data networks

Design

- [Network Security Design and Development Services](#)—Help institutions develop and integrate a strong security design
- [Incident Readiness Design Development](#)—Help institutions implement more effective incident response systems

Implement

- [Security Implementation Services](#)—Support institutions through the deployment and integration of new security technologies and processes
- [Cisco Security Agent Implementation Consulting Service](#)—Assist institutions in the implementation of the Cisco Security Agent solution

Operate

- [Incident Response Services](#)—Provide expert, real-time assistance during a network attack, available 24 hours a day, 7 days a week
- [Security Management and Monitoring Services](#)—Provide ongoing managed security support

Optimize

- [Security Optimization Services](#)—Respond more effectively to current and emerging requirements that demand changes to security infrastructure, tools, and processes

Meeting the Needs of Higher Education Networks

Colleges and universities face the same growing security threats as enterprises, with just as great a need to protect their applications, assets, and information. But unlike enterprises, academic environments have unique network requirements for openness, flexibility, and bandwidth resource control that go above and beyond those of most conventional business networks.

To address these needs, colleges and universities need robust, adaptable, state-of-the-art security solutions that address all the requirements of their diverse constituents and services. The Cisco Campus Secure program provides the sophisticated solutions in threat defense, identity management, and bandwidth control that academic environments require. These solutions are delivered under the umbrella of a unified vision of the Self-Defending Network—one that integrates security into the network architecture, combines diverse security services and solutions into a single system, and continually adapts to respond to new types of threats. Equipped with the intelligence and functionality of Cisco Campus Secure solutions, institutions of higher learning can confidently face the next generation of security challenges.

- Founded by two Stanford University graduates, Cisco Systems has maintained strong relationships with the world's leading academic institutions. Working with Cisco, colleges and universities can:
- Employ end-to-end security to protect the campus network
- Rely on proven technologies, as well as partnerships with security industry leaders, to build a Self-Defending Network
- Benefit from close collaboration among IP networking and security services, and tight integration with data, voice, video, storage, and wireless infrastructures
- Integrate and expand on security services within deployed Cisco routers, switches, and security appliances to reduce network total cost of ownership and achieve a greater return on investment
- Access the leading service and support in the industry
- Realize long-term investment protection through a commitment from Cisco Systems to the Campus Secure program and its component technologies



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)