Cisco Incident Control System

The Cisco® Incident Control System (ICS) prevents new worm and virus outbreaks from affecting businesses by enabling the network to rapidly adapt and provide a distributed response.

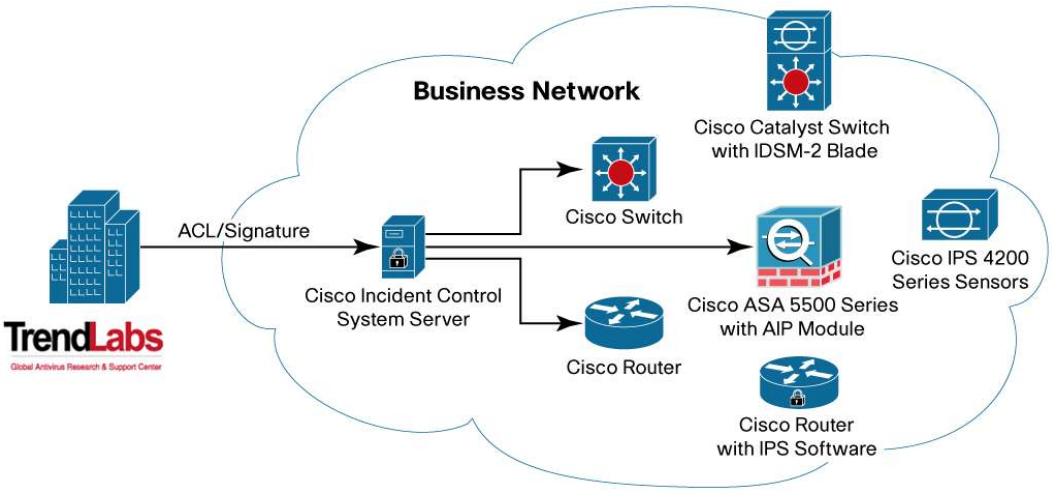
Because the time that it takes a worm or virus outbreak to spread around the world has decreased from days to minutes, a proactive response within minutes after an outbreak—regardless of its location—is necessary to help ensure the safety of business networks. The Cisco ICS solution meets that need by delivering a networkwide defense within minutes of an outbreak anywhere on the globe. In collaboration with TrendLabs, Cisco ICS uses existing Cisco Systems® network and security devices to rapidly distribute worm and virus immunization capabilities throughout the network. This fast, proactive approach prevents worms and viruses from becoming entrenched, thus helping ensure network availability and decreasing the costs associated with damage cleanup.

The primary features of the system include:

- Virus and worm-specific threat intelligence, as provided by Trend Micro, an industry-leading expert in antivirus and worm mitigation
- Rapid response, enabling proactive prevention of worms and viruses
- Empowering existing Cisco network and security devices to adapt in real time for a coordinated networkwide response
- Detailed control of how Cisco ICS mitigation policies are deployed in the business network

In Figure 1, an outbreak of malicious software identified by TrendLabs triggers a rapid response by the Cisco ICS solution, which delivers information on the threat to enable the deployment of proactive countermeasures throughout the network infrastructure.

Figure 1. Cisco ICS Antivirus and Worm Response



Rapid Proactive Prevention

Balancing the need for a quick response with quality control, the team uses a two-phase approach to prevent outbreaks from entering the network. First, a high-level policy update in the form of an access control list (ACL) is developed to stop the outbreak within minutes of its appearance. Shortly thereafter, a more granular, high-fidelity intrusion prevention system (IPS) signature that replaces the ACL is released, thus combating the emerging threat with permanent protection. The benefits of this two-phase approach are:

- A maximum level of protection within minutes after a new threat is identified.
- A more focused security stance shortly after the threat is fully characterized and a signature is made available.

After the policy or signature update is developed, it is immediately distributed using secure communications to the Cisco ICS server in the network. The server then distributes the updates to a wide variety of Cisco threat mitigation devices throughout the network. With the Cisco ICS centralized management console, the administrator has a high degree of control over the deployment of the outbreak prevention policies and signatures to the mitigation devices, including choosing either automatic or manual distribution.

This rapid response solution was designed as a complement to Cisco Services for IPS, which provides a high level of service with signatures available several hours after an outbreak as a single update file for the broad range of Cisco IPS devices, including appliances, router modules, switch modules, and Cisco IOS® Software.

Networkwide Response

Because worms and viruses are able to enter the network from many points, including intranets, extranets, branch offices, home offices, and mobile workers, a broad-based approach is required. The Cisco ICS solution works with a wide range of Cisco threat mitigation devices to cover all avenues of entry to the business network. The result is that devices across the entire network infrastructure are able to respond and adapt to the emerging threat in advance of its arrival, in a coordinated manner. This proactive networkwide approach increases the likelihood that the outbreak will be denied access or, if it finds its way in, will be rapidly contained.

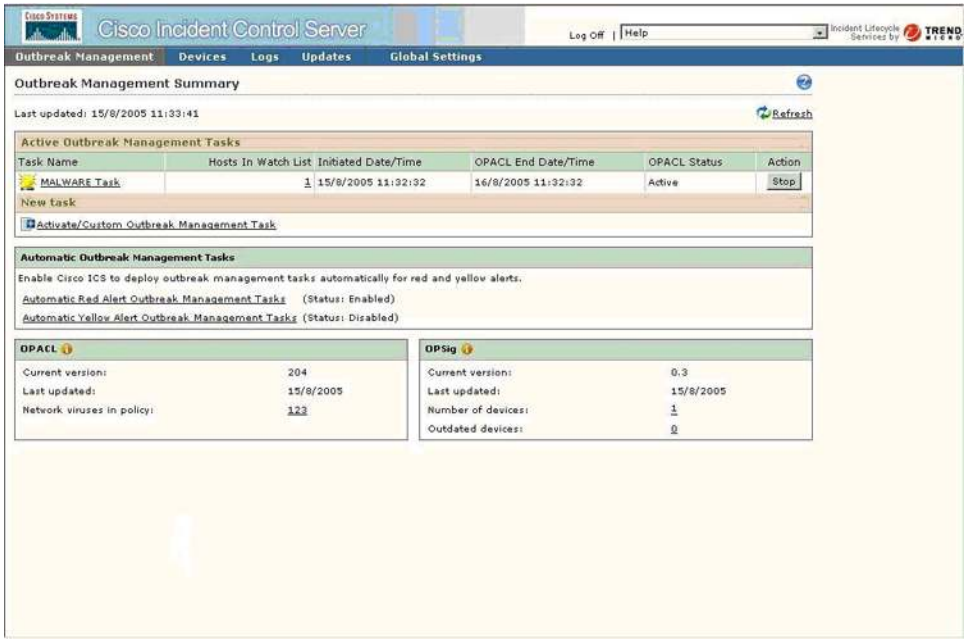
Different network and security devices offer differing levels of mitigation control. Cisco routers and switches capable of interface-based ACLs provide the base level of service supporting the broader ACL type updates that are available minutes after an outbreak. Given the breadth of Cisco network devices that support ACLs, this level of service enables protection against severe outbreaks across the entire network infrastructure. Many Cisco routers, switches, and appliances are also capable of receiving IPS signature updates. These devices deliver an advanced layer of service supporting the more detailed signature updates that are released in the second phase of the response. Devices supporting this advanced layer of service include Cisco IPS 4200 Series sensors, Cisco ASA 5500 Series adaptive security appliances (when configured with the AIP module), the Intrusion Detection System Services Module (IDSM-2) blade for Cisco Catalyst switches, and Cisco routers running a Cisco IOS Software security image. Many of these devices also support ACL-type updates, enabling a single device to provide the initial protection services of ACLs and the longer-term mitigation service delivered by IPS signatures. As part of the complete Cisco outbreak prevention solution, Cisco ICS is fully compatible with the Cisco Security Monitoring, Analysis and Response System (MARS), which helps customers readily and

accurately identify, manage, and eliminate network attacks and maintain network security compliance.

Detailed Mitigation Policy Control

The Cisco ICS server is a Web-based GUI policy server that gives administrators fine-grained control over how outbreak mitigation information is deployed in their environments. For example, administrators can define which Cisco network elements should receive ICS mitigation services, decide whether ICS services should be automatically or manually applied based on threat severity, override recommended ACL policies with locally developed ACLs, and control the types of ACLs that can be deployed to specific routers (protocol or port-specific ACLs, for example). This rich policy environment enables a high degree of local customization, helping to ensure broad protection with minimal impact to operations (Figure 2).

Figure 2. Cisco ICS Server



Specifications

System Requirements for the Cisco ICS Server

Following are the minimum versions that are required.

Operating Systems

- Windows 2000 Server or Advanced Server with SP3 (English and Japanese)
- Windows 2003 Server Standard Edition or Enterprise Edition (English and Japanese)

Web Server

- IIS: Windows 2000 IIS 5.0 or Windows 2003 IIS 6.0
- Apache: 2.0

Web Browser (for Web Console Access)

- Internet Explorer version 5.5 SP2

Hardware

- 866-MHz Intel Pentium III processor or equivalent
- 512 MB of RAM
- 350 MB of disk space

Mitigation Device License Requirements

Table 1 shows the service types available by mitigation device, and the associated licenses required to support the device.

Table 1. Mitigation Device License Requirements

Cisco ICS Coverage Type	Mitigation Device	Minimum Software Version	License Required
ACL Coverage	Cisco 800 Series routers, Cisco 1700 Series modular access routers, Cisco 1800 Series integrated services routers, Cisco 2600XM routers, Cisco 2800 Series routers, Cisco 3600 Series routers, Cisco 3700 Series multiservice access routers, Cisco 3800 Series integrated services routers, Cisco 7200 Series routers, and Cisco 7301 routers	Cisco IOS Software Release 12.3M	ICS-LIC-ACL-25
	Cisco Catalyst 3550 Series switches	Cisco IOS Software Release 12.1(22)EA5	
	Cisco Catalyst 6500 Series switches	Cisco IOS Software Release 12.2(18)SXD5	
	Cisco 7600 Series switches	Cisco IOS Software Release 12.2(17)SXB8	
ACL Plus IPS Coverage	Cisco 3800 Series integrated services routers, Cisco 7200 Series routers, and Cisco 7301 routers	Cisco IOS Software Release 12.4(4)T	ICS-LIC-IPS-HE-1
	Cisco IPS 4215 Sensor	Cisco IPS Sensor Software v5.1	
	Cisco IPS 4235 Sensor	Cisco IPS Sensor Software v5.1	
	Cisco IPS 4240 Sensor	Cisco IPS Sensor Software v5.1	
	Cisco IPS 4250 Sensor	Cisco IPS Sensor Software v5.1	
	Cisco IPS 4250XL Sensor	Cisco IPS Sensor Software v5.1	
	Cisco IPS 4255 Sensor	Cisco IPS Sensor Software v5.1	
	Cisco IDSM-2 Catalyst Module	Cisco IPS Sensor Software v5.1	
	Cisco ASA 5500 Series adaptive security appliances with AIP-SSM-20	Cisco ASA Software v7.0/ Cisco IPS Sensor Software v5.1	
	Cisco ASA 5500 Series adaptive security appliances with AIP-SSM-10	Cisco ASA Software v7.0/ Cisco IPS Sensor Software v5.1	ICS-LIC-IPS-LE-5
	Cisco 800 Series routers, Cisco 1700 Series modular access routers, Cisco 1800 Series integrated services routers, Cisco 2600XM routers, Cisco 2800 Series routers, Cisco 3600 Series routers, and Cisco 3700 Series multiservice access routers	Cisco IOS Software Release 12.4(4)T	

Ordering Information

The Cisco ICS server software must be ordered for all deployments. Additionally, one or more of the mitigation device licenses must be ordered. There is an evaluation version available for order that provides 60 days of usage and includes one of each of the ICS mitigation device licenses (Table 2).

Table 2. Ordering Information

Cisco Part Number	Description
ICS-EVAL-K9	Cisco ICS 60-Day Evaluation Kit: includes the 4 parts numbers below
ICS-SVR-V10-K9	Cisco Incident Control Server Software v1.0
ICS-LIC-IPS-HE-1	Cisco ICS License: ACL plus IPS Service for high-end devices, Qty 1
ICS-LIC-IPS-LE-5	Cisco ICS License: ACL plus IPS Service for low-end devices, Qty 5
ICS-LIC-ACL-25	Cisco ICS License: ACL Service, Qty 25

Cisco Lifecycle Services

Planning, Designing, Deploying, and Operating an Effective Cisco ICS Solution

The Cisco service portfolio provides a comprehensive range of advanced and technical support services for each stage of the customer's network lifecycle.

Cisco Advanced Services

Cisco offers advanced services, including requirements analysis, planning, design, and implementation consulting, delivering expert advice essential to an effective Cisco ICS solution. Cisco Advanced Services consultants provide the following services to help ensure your Cisco ICS deployment is a success:

1. Cisco Incident Control System Readiness Assessment
2. Cisco Incident Control System Design Development
3. Cisco Incident Control System Implementation Engineering

Cisco Technical Support Services

The Cisco Technical Support Services portfolio includes Cisco Software Application Support plus Upgrades (SASU) to address support requirements for Cisco ICS server software. Cisco SASU features include access to Cisco ICS software updates, the Cisco Technical Assistance Center, and Cisco.com around the clock, anywhere in the world.

It is a requirement of the Cisco ICS solution that all mitigation devices must be covered by an active support contract. Mitigation devices receiving ACL coverage must be covered by an active Cisco SMARTnet® contract. Mitigation devices receiving IPS coverage must be covered by an active Cisco Services for IPS contract.

Resources

For more information about Cisco ICS, visit http://www.cisco.com/go/ics.

For more information about Cisco IPS solutions, visit http://www.cisco.com/go/ips.

For more information about Cisco Technical Support Services, visit http://www.cisco.com/go/tss.

For more information about Cisco Advanced Services, visit http://www.cisco.com/go/securityconsulting.

\

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 (USA) Pte. Ltd.
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.**

Printed in USA C78-446468-00 12/07

