



TECH TALK:

COMBATING BLASTER AND OTHER INTERNET WORMS

TOP 100 QUESTIONS AND ANSWERS

1. HOW DOES A WORM GET THROUGH A FIREWALL?

Unfortunately, worms propagate by appearing as normal network traffic. For example, if a firewall allows access to a Web server via HTTP (TCP port 80), and the worm appears to be a valid HTTP request, then the worm traffic flows through to the server. To effectively combat worms, you should use intrusion detection products or other content inspection engines (such as Network-Based Application Recognition [NBAR]).

2. WILL THE BLASTER WORM COME BACK AFTER YOU HAVE SOLVED THE PROBLEM?

The Blaster worm will linger for some time, and may continue to interfere with normal functioning. We recommend using the Microsoft patch and implementing the best practices described in the Cisco® Product Security Incident Response Team (PSIRT) announcement:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

For additional information, please see the SAFE Blueprint from Cisco response at:

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

3. NBAR WAS EFFECTIVE AGAINST CODE RED. IS IT APPROPRIATE FOR USE AGAINST CURRENT WORMS?

NBAR is effective as a tactical tool to block malicious packets while you are patching or otherwise establishing defenses against a worm. It does require some type of match value that is unique to the worm. For example, with Code Red we can use an HTTP match on default.ida. With Blaster, we look for SQL packets of a specific length.

4. HOW CAN YOU TELL IF YOU HAVE BEEN INFECTED BY THE BLASTER WORM?

You can tell whether your computer has been infected by the Blaster worm by looking at your Windows XP and 2000 systems. Look at processes in the Task Manager. If you see MSBlaster in the list, you are infected. Download the patch from the Microsoft site, and implement the Cisco changes described in:

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

5. WHAT IS THE DIFFERENCE BETWEEN A VIRUS AND A WORM?

A virus is a piece of code that attaches itself to another document or program and executes when that document or program is opened. A worm is typically a self-contained program that can infect other systems on its own and then copy itself over and continue the infection. Like their biological equivalents, viruses require “vectors”—something to carry them from one system to another.

6. CAN BLASTER AND SUBSEQUENT WORMS BE BLOCKED USING FIREWALLS TO PROTECT HOSTS OR NETWORK DEVICES?

Yes. For more details, visit:

<http://www.cisco.com/warp/public/707/cisco-sn-20030814-blaster.shtml>

7. IS THE USE OF PERSONAL FIREWALLS RECOMMENDED (IN CONJUNCTION WITH ANTIVIRUS TOOLS) TO BLOCK WORMS?

A personal firewall alone would not be effective in stopping exploitation of an application that is allowed to use the network. For example, the Blaster worm targeted Microsoft file sharing, which (in a corporate environment) is frequently an authorized function. Intrusion prevention (for example, as provided by the Cisco Security Agent) will prevent authorized applications from being subverted by a "Day Zero: attack."

8. HOW EFFECTIVE WAS THE CISCO HOST-BASED INTRUSION DETECTION SYSTEM (HIDS) SOLUTION IN FINDING, ALERTING, AND ELIMINATING THE BLASTER WORM AND ALL ITS VARIATIONS?

Cisco HIDS was very effective in (part of the Cisco Security Agent) detecting, alerting, and most importantly, preventing the compromise of hosts. Cisco Security Agent default policies provided protection against Blaster and all of its variants, without requiring system administrators to download updates or signatures.

9. HOW DO YOU PROTECT YOUR NETWORK FROM INFECTED MACHINES CONNECTING THROUGH A VPN?

The best way to protect your VPN is to terminate the tunnel in front of the firewall and then block the port, as described in the Cisco Product Security Incident Response Team (PSIRT) announcement—135, 444, and UDP 69. This should keep the worm from spreading further. Make sure to apply the Microsoft patches.

10. CAN REGULARLY SCHEDULED ANTIVIRUS AND ANTIWORM SCANS, OR UPDATES TO THE OPERATING SYSTEM (OS) PROVIDE ADEQUATE PROTECTION TO OUR NETWORK?

Antivirus scans are only effective against known attacks, so there is a lag between when an attack is launched and when an update becomes available. OS updates are only effective against known vulnerabilities. Sometimes patches cause applications to cease normal functioning, so testing is critical to prevent a self-imposed denial of service (DoS) from a poorly tested patch.

11. IS THERE A MICROSOFT SECURITY PATCH THAT IS CUMULATIVE, OR DO I HAVE TO FIND EACH INDIVIDUAL PATCH?

You would need each individual patch.

12. IS IT FEASIBLE TO SAY THAT A WORM THAT COULD PATCH NUMEROUS SYSTEMS WOULD BE A GOOD THING? SHOULD AN ORGANIZATION BE CREATED TO ADDRESS THESE THINGS?

In general, it could be a good thing, but in most cases, especially the case of Blaster, the good worms reboot the system. This has led to people losing unsaved data on their computers. I would be surprised to hear that someone is trying to figure out how to do this and not affect the end user.

13. HOW CAN WE GET THE MOST CURRENT SECURITY INFORMATION FROM CISCO DURING A VIRUS EVENT?

The Cisco Product Security Incident Response Team (PSIRT) provides the most current information regarding network security issues, fixes, etc., as they apply to Cisco products. For more information, visit:

<http://www.cisco.com/warp/public/707/advisory.html>

14. WHAT IS THE BEST WAY TO PROTECT THE HOST COMPUTER WHEN USING THE VPN CLIENT WITH A DIAL-UP ACCOUNT?

Cisco Security Agent works with the virtual private network (VPN) client (via Are You There [AYT]). The VPN can make sure that Cisco Security Agent is present before the tunnel is enabled. Cisco Security Agent provides protection against Blaster and other worms.

15. HOW ARE INTERNET WORMS SPREAD FROM ONE LOCATION SO RAPIDLY?

Worms replicate themselves exponentially. First one machine is infected, then two, then four, then sixteen. Once infected, all machines spread to several other machines. Keep an eye on security advisories and patch appropriately as soon as possible.

16. WHAT IS A TROJAN HORSE?

A Trojan horse is a malicious, security-breaking program that is disguised as something benign.

17. HOW CAN WE TELL IF "BACK DOORS" HAVE BEEN SET UP ON OUR SYSTEMS?

There are various software packages that you can use to determine if a "back door" has been set up on your systems. One simple way is to use a port scanner to scan your systems and look for any open ports that are not normally open. This requires you to have a good knowledge of the ports that should normally be open on your system.

Other software to consider would be Nessus, which can identify potential back doors. You can also investigate the CHK rootkit open source software at:

<http://www.chkrootkit.org>

18. IS THERE AN EFFECTIVE WAY TO PROTECT LEGITIMATE TRAFFIC FROM TRAFFIC THAT MAY BE GENERATED FROM AN INFECTED SYSTEM?

Infected systems should have their switch ports disabled, prompting a quarantine until they have been cleaned. A Cisco Network Intrusion Detection System (IDScan) prevent malicious traffic automatically. Make sure that Signature Update 51 has been installed on the Cisco IDS.

19. BECAUSE OF THE SHEER VOLUME OF MICROSOFT PATCHES THAT ARE RELEASED, AND BECAUSE TESTING MUST BE DONE BEFORE PATCHING TAKES PLACE ON PRODUCTION, NETWORK ADMINISTRATION HAS BEEN DIFFICULT. HAS ANYONE DISCOVERED INTELLIGENT WAYS TO MANAGE THE PATCH PROCESS?

Patch management is a huge problem for two reasons:

1. The volume of patches (and the urgency of security patches) forces emergency update efforts. This is expensive and disruptive.
2. Some patches cause critical applications to fail. This forces a choice between remaining insecure and causing application failure. An in-depth defense that blocks "Day Zero: attacks" (such as Cisco Security Agent) does not remove the need to patch, but does allow a longer period to test the patch to ensure that it is safe. By protecting against attacks before the patch can be deployed, patching efforts can be addressed in a more organized manner.

20. IN TERMS OF MITIGATION METHODOLOGY, IS IT MORE IMPORTANT TO IDENTIFY THE WORM OR TO CONTAIN IT?

You should contain the infection as quickly as possible. Identification of the worm is the next step, once you have stopped the infection from spreading in your network or beyond.

21. MY COMPANY USES PORT 135 TO RUN A PRIVATE APPLICATION. WHAT CAN I DO WITHOUT STOPPING THIS COMPANY PROCESS?

In cases where access to well-known ports, such as TCP/UDP 135, is required for remote sites via the Internet, VPN technology may provide a more secure solution. For details, please see:

http://www.cisco.com/en/US/netsol/ns110/ns170/net_solution_home.html

22. BLOCKING PORT 135 IS FINE FOR CONTAINING THE WORM, BUT IT DISRUPTS SOME WINDOWS 2000 SERVER FUNCTIONS. WITH HUNDREDS OF SERVERS ON THE NETWORK, ACCESS CONTROL LISTS (ACLs) ARE DIFFICULT TO MANAGE. IS THERE A BETTER WAY TO DEFEND AGAINST WORMS THAT EXPLOIT NECESSARY PORTS AND SERVICES?

Cisco Security Agent allows you to block any ports on hosts. However, blocking attacks on ports is not the only method of preventing damage. Cisco Security Agent provides "in-depth defense" by providing layers of protection. For example, Cisco Security Agent prevented Blaster from spawning a command shell and executing its payload.

23. HOW DOES CISCO SECURITY AGENT DIFFER FROM PERSONAL FIREWALLS SUCH AS ZONE ALARM?

Cisco Security Agent provides personal firewall capabilities (port blocking, for example). However, it also protects



applications that are allowed to communicate on the network, such as Web browsers and e-mail clients. Worms that target vulnerabilities in these desktop applications can be mitigated with Cisco Security Agent.

24. WILL THE CURRENT PATCH FOR THE BLASTER WORM DETECT AND REMOVE VULNERABILITIES FOR THE VARIANTS?

Yes. The current patch for the vulnerability that the Blaster worm exploits also prevents infection from any worm variants. The vulnerability is the same across the variants; one patch will stop Blaster and its variants.

25. IF AN INFECTED HOME COMPUTER IS CONNECTED TO OUR COMPANY NETWORK THROUGH A VPN, CAN THE WORM SPREAD TO THE COMPANY NETWORK?

If the home computer is infected when it connects to the virtual private network (VPN), then yes, it is possible. As shown on the SAFE Blueprint from Cisco, we recommend placing remote-access VPN resources into a data management zone (DMZ) to allow traffic inspection of VPN traffic (post-decryption), prior to its accessing the network.

26. OUR NETWORK WAS INFECTED BY THE WELCH WORM ON MONDAY MORNING, AND SYMANTEC RELEASED THE FIX ON TUESDAY AFTERNOON. WHAT DO WE DO WHEN THERE IS NO FIX AVAILABLE YET?

Antivirus scanners only protect against known attacks, for which a signature has been created and deployed. Other approaches (for example, Cisco Security Agent's behavior analysis) must be used to stop new attacks, for which there is no signature.

27. WHAT IS NBAR?

Network-Based Application Recognition (NBAR) is a feature built into Cisco routers that allows traffic to be marked, according to whether it is application- or service-specific, and then dropped, shaped, or policed, using various quality of service (QoS) or access control list (ACL) mechanisms. For more information, see:

<http://www.cisco.com/warp/public/732/Tech/qos/nbar/>

28. IS CISCO SECURITY AGENT STAND-ALONE SOFTWARE THAT ACTS WITHOUT REFERRING TO A SERVER?

Cisco Security Agent is not a stand-alone product. It is centrally managed from the Cisco management console, which is called CiscoWorks VPN/Security Management Solution (VMS).

29. DOES THE BLASTER WORM AFFECT INDIVIDUAL HARD DRIVES?

No. Blaster installs itself in a system directory and runs from there. It does not spread to other disks, only other computers.

30. CAN A PC BE PROTECTED AGAINST A WORM IF IT IS TURNED OFF WHEN NOT IN USE?

The attack window for that worm can certainly be reduced. Any time a machine is unavailable, it cannot be infected. However, depending on the downtime of the machine to prevent infection is a poor strategy—this could interfere with other mitigation and prevention strategies, like regularly scheduled updates at a certain time of day.

31. WHAT ARE INTERNET SERVICE PROVIDERS DOING TO HELP PREVENT THE SPREAD OF THESE ATTACKS?

Different service providers have different approaches to handling denial-of-service (DoS) attacks in general; the best source of information on this subject is the specific service provider you are using.

32. IS THERE A WAY TO USE PRIVATE VIRTUAL LANs (VLANs) TO CONTAIN A WORM WITHIN YOUR NETWORK?

Private VLANs can contain a worm just to that VLAN. Standard Layer 2 VLANs are subject to infection, as they provide no filtering of data. Best bets are to install the patch and check the following URLs to see what can be done from a network perspective:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml



33. WILL CISCO SECURITY AGENT BLOCK VALID REQUESTS OR ACTIONS BY LEGITIMATE PROGRAMS?

This is a policy-tuning issue, and there are tools to assist you in this tuning, such as the profiler feature.

34. HOW DO I DEPLOY CISCO SECURITY AGENT ON MY NETWORK?

Cisco Security Agent can be deployed on your network in several ways. You can bury it in a login script, distribute it through traditional methods such as SMS, e-mail an executable, or have the end user go to a Web page and download the executable. You could also manually install it with a CD.

35. WOULD DILIGENT PATCHING PROCEDURES HAVE HELPED PREVENT BLASTER AND ITS VARIANTS FROM SPREADING? WHAT PRODUCTS, ASIDE FROM WINDOWS AUTO UPDATE, CAN HELP WITH PATCHING?

Diligent patching is always recommended, but is often administratively cumbersome. If just one new patch comes in each week, can your network productivity sustain the downtime required to apply and reboot the patch? One strong argument for implementing Cisco Security Agent is the ability to manage and modify profiles immediately, to protect servers from "time zero," while allowing you to adopt a routine as opposed to a reactive patching schedule.

36. WHAT IS THE DIFFERENCE BETWEEN NBAR AND CISCO IDS WHEN DEALING WITH WORMS?

Network-Based Application Recognition (NBAR) is a mechanism for marking network traffic based upon application- and service-specific information. Cisco Intrusion Detection System (IDS) products provide detection and notification of potentially undesirable activity on the network.

37. CAN CISCO SECURITY AGENT INTERFERE WITH THE NORMAL DAY-TO-DAY OPERATION OF A SERVER? FOR EXAMPLE, COULD IT POSSIBLY PREVENT SOMETHING FROM HAPPENING THAT SHOULD HAPPEN?

Cisco Security Agent policies have been carefully constructed to avoid blocking legitimate activity. It is also easy to tune the policies to the local environment. Agents can run in "Testmode," which alerts but does not block behavior. The policy-tuning wizard helps to automate policy tuning so that policies are adapted in a sensible, best-practices manner.

38. WILL CISCO SECURE IDS SLOW DOWN OUR NETWORK IF FULLY IMPLEMENTED?

Network-based Cisco Secure IDS is passive and will have no effect on your network. Host-based Cisco Security Agent will add three-percent CPU usage to a host or server, but so far, has stopped all of the major worms—Blaster, Code Red, Nimda, and Slammer.

39. AM I EXPOSED TO THIS BLASTER WORM IF I DO NOT BLOCK OUTBOUND CONNECTIONS VIA THE FIREWALL OVER THE RECOMMENDED PORTS?

Yes. These worms (Nachi or Blaster) may make inbound connection attempts against your network; therefore, you need to block these ports inbound as well. For more information on filtering, please refer to the SAFE Blaster mitigation white paper at:

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

40. WHAT'S THE BESTWAY TO FIND CISCO CONSULTANTS OR TECHNICIANS IN MY AREA?

The Cisco Partner Locator Tool at Cisco.com can be used to locate resellers and partners in your area:

http://tools.cisco.com/WWChannels/LOCATR/jsp/partner_locator.jsp

41. WHAT IS CISCO NETFLOW?

Cisco NetFlow is a technology that allows a user to see network flows, or conversions, as they pass through Cisco

routers and switches. This technology has many uses in the fields of traffic characterization and anomaly detection. For more details, see:

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

42. HOW DO I OBTAIN A COPY OF CISCO SECURITY AGENT?

To obtain a copy, request an evaluation of CiscoWorks VPN/Security Management Solution V2.2, (VMS) which includes the Cisco Security Agent software:

<http://www.cisco.com/cgi-bin/tablebuild.pl/vms>

You can also request a Cisco Security Agent evaluation license key:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl>

43. WHICH IS PREFERABLE FOR A GROUP OF FEWER THAN 35 SERVERS—CISCO SECURITY AGENT OR OKENA STORMWATCH?

Cisco Security Agent Version 4.0 is the latest version of Okena StormWatch. StormWatch 3.2 is no longer available.

44. WHAT ARE THE MAIN POINTS FOR INTRUSION DETECTION THROUGHOUT THE SYSTEM?

The SAFE Blueprint team at Cisco will be delivering a document on intrusion detection best practices very soon. Please check:

www.cisco.com/go/safe

45. WE HAVE MANY USERS WHO ACCESS WINDOWS SHARES THROUGH AN INTRANET FIREWALL. THEY KEEP LOSING AND REGAINING ACCESS TO THOSE SHARES. COULD THIS BE A SIGN OF VIRUS OR WORM ACTIVITY?

To determine whether or not these are signs of a virus or a worm, you need an intrusion detection system (IDS) to look into the payloads of these packets. In general, it is not a good idea to access Windows shares through a firewall, unless both sides of that firewall are trusted subnets.

46. DOES CISCO IDS HAVE AN AUTOMATIC PROCESS IN GETTING THE SIGNATURES?

Yes. Cisco IDS sensors can be set up to download their service packs at preset times through the Cisco IDS MC under CiscoWorks VPN/Security Management Solution (VMS).

47. WOULD BLOCKING PORTS 135 AND 139 ON UDP AND TCP AFFECT USERS REMOTELY CONNECTED TO THE NETWORK VIA A VIRTUAL PRIVATE NETWORK (VPN)?

Yes. It would affect the ability of users to access Windows network services. Some of these service locations will be cached from the time the user is directly connected to the local network versus over the VPN. You may also consider hard-coding this information in the LMHOSTS file.

48. IS CISCO SECURITY AGENT AVAILABLE FOR DOWNLOAD?

Yes. You can download Cisco Security Agent at the following site:

<http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>

49. HOW IS CISCO SECURITY AGENT LICENSED?

Cisco Security Agent is licensed by machine (servers and desktops). A CiscoWorks VPN/Security Management Solution (VMS) 2.2 license is also required for the management of Cisco Security Agent hosts.

50. IS THERE ANY SOFTWARE THAT WILL WARN OF AVIRUS COMING BEFORE IT HITS ANY DEVICE ON THE NETWORK?

7

Not really. There are network antivirus vendors, but they are signature-based. The best option would be something like Cisco Security Agent. It looks at the behavior of a CPU and stops potentially dangerous events. This is called Day Zero protection. It has stopped all major viruses on the first day—Blaster, Code Red, Nimda, and Slammer.

51. WILL AN INTRUSION DETECTION SYSTEM (IDS) STOP AN ATTACK FOR WHICH IT DOES NOT HAVE A SIGNATURE?

Yes, if one of the protocol anomaly engines detects it and you have a response enabled.

52. CAN THE CISCO SECURITY AGENT COEXIST PEACEFULLY WITH ANTIVIRUS SOFTWARE ON THE DESKTOP? DO THEIR FUNCTIONS OVERLAP?

Cisco Security Agent coexists with antivirus scanners. Each does a different job—antivirus scans for known virus patterns; Cisco Security Agent blocks new worms and viruses for which there is no signature.

53. SIMPLY STATED, HOW DO NETWORK-BASED INTRUSION DETECTION SYSTEMS (NIDS) DIFFER FROM HOST-BASED INTRUSION DETECTION SYSTEMS (HIDS)? HOW DO THEY COLLABORATE?

NIDS monitors traffic in transit through a point on the network, while HIDS monitors traffic received by a specific host to which it is applied. Both HIDS and NIDS focus on detecting malicious network traffic, but HIDS can also monitor the intended effect of a received packet upon critical processes. They can collaborate by providing events to a common analysis engine, which the Cisco Security Agent and Cisco NIDS products do in sending alerts to CiscoWorks VPN/Security Management Solution (VMS) security monitor.

54. ARE WIRELESS DEVICES MORE VULNERABLE TO VIRUSES?

No. Viruses have no concept of the network types that lie underneath them.

55. IS THERE A SMALL-BUSINESS VERSION OF CISCO SECURITY AGENT AVAILABLE?

Cisco Security Agent is scalable for small and medium-sized businesses. It is a centrally managed product for desktops and servers.

56. IF EVERYONE INCREASES THEIR PROTECTION, WON'T THAT JUST FORCE THE NEXT VIRUS TO BE MORE CLEVERLY WRITTEN?

That is certainly a possibility. But the idea is that you do not want to be an easy target. Viruses typically pick a few infection vectors to be effective. If you remove these vectors, then you are safe, at least from that particular virus. For example, you lock your car doors not because it is the ultimate protection but because it forces a thief to go the extra steps to pick the lock or to break a window. The same is true of network security. You do not want to be an easy target. Implement in-depth security and at least make the virus writers work at it, as opposed to leaving the front door wide open.

57. WHAT EFFECT DOES BLASTER HAVE ON UNIX SYSTEMS?

Only Windows-based systems (2000, NT, XP, 2003) were vulnerable to the exploit that Blaster used. However, high traffic load in local network segments could lead to slow response times.

58. WHY DOES IT APPEAR THAT MACINTOSH COMPUTERS, OR MACS, ARE NOT AFFECTED BY ALL THESE WORMS?

Most of the recent worms have specifically targeted Microsoft services and use Intel-compiled Windows executable code to cause damage. Therefore, Mac users are less likely to be affected by these events.

59. WAS BLASTER RELATED TO THE REMOTE-PROCEDURE CALL (RPC) EXPLOIT?

Yes. The Blaster worm exploited the vulnerability described in Microsoft Security Bulletin MS03-026.

60. WHAT ABOUT INTRUSION BY A WORM THROUGH A FIREWALL VIA THE SECURE PORT 443 TO AN INTERNAL WEB SERVER?

8

Attacks via an encrypted channel can be blocked by one of two methods:

1. Terminate the Secure Sockets Layer (SSL) session before the server, offloading the encryption, decryption and monitoring for attacks in plain text on a network device. 2. Add software agents, such as Cisco Security Agent on the server, which will block malicious behavior sent via encrypted attack.

61. HOW DOES CISCO SECURITY AGENT SOFTWARE PREVENT BLASTER WITHOUT NEED OF AN UPDATED SIGNATURE? DOES CISCO SECURITY AGENT HINDER NORMAL OPERATING SYSTEM (OS) ACTIVITY?

Cisco Security Agent provides effective protection against new and unknown attacks because Cisco Security Agent default policies are designed to prevent malicious activities exhibited by Trojan horses, worms, and viruses. Default policies do not hinder normal OS activities.

62. IF THE PORTS ARE NOT OPEN, DO WE STILL NEED TO WORRY ABOUT ENTRY THROUGH A FIREWALL?

Some known attacks and code can tunnel traffic through nontraditional transports, such as a LOKI tunnel. Most likely, you will be okay, but this is never guaranteed.

63. WHERE CAN I FIND THE CODE TO BLOCK PORTS 135, 139, AND 445 (TCP/UDP) ON A CISCO PIX FIREWALL?

By default, the Cisco PIX® Firewall blocks all inbound traffic from an interface with a lower security value destined for an interface with a higher security value. You do not need to specifically block these ports on the Cisco PIX Firewall—they are denied by default.

64. HOW DOES CISCO SECURITY AGENT WORK TO FIGHT WORMS?

Cisco Security Agent recognizes suspicious activity, such as buffer overflows, or writes to the system directory or the registry. It will stop this action at the CPU kernel level, and the worm cannot place itself on the machine.

65. WHY WOULD I USE CISCO SECURITY AGENT INSTEAD OF A FIREWALL?

If you need only a personal firewall, Cisco recommends using Cisco Security Agent instead—you still get firewall capability, but you also get prevention. If you are referring to a hardware firewall, then Cisco Security Agent is complementary (meaning that you should have both).

66. AS AN ISP, WITHOUT THE ABILITY TO LOOK AFTER EVERY COMPUTER ON OUR NETWORK, WHAT IS THE BEST WAY TO FIND INFECTED MACHINES?

Many of our ISP customers make use of Cisco NetFlow in conjunction with anomaly-detection systems provided by Cisco Partner companies, in order to rapidly detect denial of service (DoS) or worm-type traffic. For details, see:

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

and:

<http://www.arbornetworks.com>

67. WE HAVE A CISCO PIX 506 FIREWALL. HOW DO I FIND OUT IF THERE ARE PATCHES AVAILABLE FOR IT?

Please refer to the Cisco Software Center at:

<http://cisco.com/public/sw-center/>

68. IS IT POSSIBLE THAT A WELL-WRITTEN WORM MIGHT INFECT MANY MACHINES WORLDWIDE WITH NO VISIBLE EFFECT TO THE USERS?

Yes.



THIS IS THE POWER OF THE NETWORK. **now.**

69. WILL CISCO SECURITY AGENT BLOCK AN INFECTED LAPTOP FROM PROPAGATING A WORM WHEN THE USER RECONNECTS TO THE CORPORATE LAN?

9

Cisco Security Agent will stop a laptop from getting infected, whether it is connected directly or remotely to the organization's network.

70. CAN THE CISCO SECURITY AGENT DESKTOP CLIENT BE MODIFIED ON THE HOST, OR IS IT A PUSH TECHNOLOGY FROM A CENTRAL SERVER?

The Cisco Security Agent desktop client is actually updated when it polls into the management console.

71. HOW DO YOU ACQUIRE CISCO SECURITY AGENT?

To obtain a copy, request an evaluation of CiscoWorks VPN/Security Management Solution (VMS) 2.2, which includes the Cisco Security Agent software:

<http://www.cisco.com/cgi-bin/tablebuild.pl/vms>

You can also request a Cisco Security Agent evaluation license key:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl>

72. I HAVE A CISCO PIX 515R. WHERE SHOULD I INSTALL THE CISCO SECURITY AGENT?

The Cisco Security Agent would be installed on hosts behind the firewall.

73. HOW WAS IT POSSIBLE THAT A COMPUTER BECAME INFECTED WITH BLASTER EVEN WITH THE RPC PATCH?

The virus can hit the patched PC, but it will have no effect.

74. IF YOU INSTALL ALL MICROSOFT PATCHES, UPDATE YOUR ANTIVIRUS SOFTWARE DAILY, AND USE A FIREWALL, CAN YOU SAY THAT YOU ARE SAFE FROM WORMS AND VIRUSES?

Overall the answer is yes. However, be aware that even if you keep up to date on all of Microsoft patches, new vulnerabilities are constantly being discovered and not all vulnerabilities are published. It is remotely possible for a worm to exploit a vulnerability for which Microsoft does not have a patch.

75. CAN WORMS AFFECT UNIX/AIX?

Yes. However, there are factors that often prevent those platforms from being targeted. For example, the number of Windows-based platforms is much greater, so the probability of writing a scripted attack and locating a vulnerable host is much greater, as opposed to UNIX/AIX.

76. IS THERE AN EXAMPLE OF USING NBAR AGAINST THE CODE RED VIRUS?

Network-Based Application Recognition (NBAR) is very effective against Code Red. For more information about using NBAR against Blaster, see the SAFE white paper on Blaster at:

<http://www.cisco.com/go/SAFE>

77. WILL THE CURRENT PATCH FOR THE BLASTER WORM DETECT AND REMOVE VULNERABILITIES FOR THE VARIANTS?

It will stop variants that use the same exploit in the attack. It will not stop variants that use new attacks.

78. IS THERE A CISCO SECURITY AGENT OR HOST-BASED INTRUSION DETECTION SYSTEMS (HIDS) FOR UNIX?

Cisco Security Agent is supported on Solaris 2.8.



THIS IS THE POWER OF THE NETWORK. **now.**

79. DO YOU ANTICIPATE MORE ATTACKS ON UNIX PLATFORMS?

Most software, whether for an application or an operating system, will have vulnerabilities that could be potentially exploited. UNIX-based systems will be susceptible, as well.

80. EACH TIME A VIRUS OR WORM HAS BEEN RELEASED, IT HAS BEEN MORE DANGEROUS AND DESTRUCTIVE THAN THE LAST. GIVEN THE HISTORY OF PREVIOUS VIRUSES AND WORMS, CAN AN ADMINISTRATOR ANTICIPATE ANYTHING REGARDING THE NEXT VIRUS OR WORM?

While worms always use new exploits, they are remarkably similar in the malicious behavior they attempt. Many try buffer overflows, execution of shell code, downloading and executing code from the network, or accessing e-mail address books. Blocking these common, malicious behaviors will stop new worms. The Cisco Security Agent default policies are designed to address this.

81. CAN CISCO PRODUCTS PREVENT OR BLOCK GNUTELLA CLIENTS FROM TRAVERSING THE NETWORK?

Cisco Security Agent can control which desktop applications are allowed to be network clients or servers. This lets you control any peer-to-peer application, including Gnutella.

82. VIRUSES SUCH AS LOVEGATE PROPAGATED VIA SHARED FOLDERS ACROSS THE NETWORK. WHAT IS THE BEST WAY TO DEFEND AGAINST THESE TYPES OF VIRUSES?

The propagation technique might vary, but the tools to mitigate the spread are typically the same. In this case, the recommendation would be to use Cisco Security Agent in conjunction with antivirus protection.

83. IS IT TRUE THAT VPN TUNNELING CAN BYPASS A HARDWARE FIREWALL, SO YOU COULD BE PROTECTED FROM THE INTERNET, BUT INFECTED BY SOMEONE INSIDE THE COMPANY OVER THE TUNNEL.

Yes, the Cisco Security Agent works with the Cisco VPN client via "Are You There" (AYT). You can configure the VPN not to enable the tunnel if Cisco Security Agent is not present on the remote system. Cisco Security Agent will protect the remote system.

84. HOW CAN A NETWORK BECOME INFECTED IF THE RECOMMENDED PORTS ARE NOT OPEN ON THE EDGE FIREWALL?

It's possible that someone may have brought an infected host into the environment. For example, this could occur over the LAN with a laptop brought in from a remote site, or there is a possibility that someone with infected hosts is using your wireless LAN (WLAN). To mitigate the multiple methods worms can use to spread themselves in your environment, you must follow a layered approach to security. For best practices on how to accomplish this, please refer to the SAFE Website at:

<http://www.cisco.com/go/safe>

85. CAN WE BUILD OUR OWN SIGNATURES? WHERE WOULD WE START?

Yes, you can build custom signatures. They can be an important part of your worm mitigation tool kit. More information on custom signatures can be found on the Cisco Intrusion Detection System (IDS) site.

<http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html>

86. DOES CISCO SECURITY AGENT REQUIRE A LEARNING PERIOD TO SET UP A POLICY?

Cisco Security Agent ships with out-of-the-box security policies that can be applied across your servers and desktops right away. The Cisco Security Agent Management Console has an event wizard, making it very easy to tune default policies to unique environments. Writing your own custom policies does require a learning period.

87. WE HAVE JUST DOWNLOADED THE NEW VERSION OF CISCO VMS AND CERTIFICATE AUTHORITY FROM CISCO.COM. ON THE CERTIFICATE AUTHORITY, IS IT BEST TO RUN THE DEFAULT, OR SHOULD WE BE LOOKING AT TRAFFIC FLOWS NOW?

Cisco Security Agent looks at application behavior, not traffic flows. You would want to tune the Cisco Security



THIS IS THE POWER OF THE NETWORK. **now.**

Agent policies as required in your environment, and use NIDS to monitor traffic flows.

88. DOES CISCO PIX TECHNOLOGY PROTECT AGAINST WORMS IF THE SESSION IS ESTABLISHED FROM INSIDE, SUCH AS VIA BROWSING?

No. If the session is initiated from the inside and the worm uses the browser connection to download itself to the target system then, the Cisco PIX® system will not be able to stop it.

89. CAN YOU BE INFECTED FROM GNUTELLA SERVICES? HOW CAN YOU BLOCK THESE CLIENT APPLICATIONS?

Cisco IDS can take actions to prevent these traffic types. This requires Cisco Intrusion Detection System (IDS) Version 4.1 with Signature Update 49.

90. CAN BLASTER BE TRANSMITTED THROUGH A VIRTUAL PRIVATE NETWORK (VPN) CONNECTION?

Yes. You will want to ensure that you have protection on the end point if you are going to allow it in via VPN.

91. IS CISCO SECURITY AGENT THE SAME AS THE HOST-BASED INTRUSION DETECTION SYSTEM (HIDS) THAT CISCO ACQUIRED FROM OKENA?

Yes, the two are the same, but Cisco Security Agent offers some enhancements and product integration.

92. CAN CISCO INTRUSION DETECTION SYSTEM (IDS) BE SET UP TO AUTOMATICALLY CONFIGURE CISCO PIX 515 FIREWALL TO BLOCK AND KILL A SUSPECTED CONNECTION?

Yes. The Cisco IDS sensor can be configured on a per-signature basis to use the shun command on the Cisco PIX Firewall system to block and kill suspected connections.

93. WOULD SOME OF THESE WORMS CAUSE YOUR COMPUTER TO TRY TO CONNECT TO THE INTERNET BY ITSELF AND KEEP YOU FROM DOWNLOADING ANTIVIRUS UPDATES?

They can definitely cause the computer to connect to the network by itself as it infects other machines. If you think you have this problem, the best thing to do is delete nsblast.exe and then delete any reference to msblast from your registry.

94. HOW DO YOU FIND THE WORM ON LOW-END ROUTERS OR SYSTEMS WHERE CISCO IOS® SOFTWARE DOES NOT SUPPORT NBAR?

For Cisco 2600Xm and 3700 series routers, you can use the Cisco Intrusion Detection System (IDS) network module.

95. THESE WORMS CREATE HAVOC ON OUR NETWORK. DOES CISCO HAVE A WEBSITE WHERE I CAN GO AND FIND WHAT PORTS NEED TO BE BLOCKED?

The best thing to do in the midst of a critical situation is to visit the Cisco Product Security Incident Response Team (PSIRT) Website:

www.cisco.com/go/psirt

Other vendors provide similar sites, such as:

www.microsoft.com/technet

96. DOES CISCO POLICY MANAGER ALLOW FOR MASS CHANGES TO ROUTERS OR FIREWALLS TO HELP IN QUICK ACLS?

This can be accomplished using CiscoWorks VPN/Security Management Solution (VMS) Software (Cisco PIX Management Console).

97. WE ARE CURRENTLY COMBATING THE BLASTER. WE HAVE SITES WHERE SOME CAN TELNET TO THE SERVER AND SOME CANNOT. IS THIS A SYMPTOM OF THE WORM?

12

No. This is not a symptom of the worm, if this is happening at the same time. If access to the server is not possible at different times, this could be symptomatic of the worm, because the worm can cause servers to reboot.

98. IS CISCO SECURITY AGENT AN UNLIMITED LICENSE WITH CISCOWORKS VPN/SECURITY MANAGEMENT SOLUTION VMS 2.2?

Cisco Security Agent is licensed by the number of servers or desktops protected. One Cisco Security Agent Management Center (running on Cisco VMS 2.2) supports 5,000 agents.

99. WHEN WILL CISCO EXPAND NETWORK-BASED APPLICATION RECOGNITION (NBAR) TO OTHER PLATFORMS BESIDES THE CISCO 7200 SERIES?

NBAR is available on several Cisco platforms, including the 3600, 3700, 7200, and 7500 series.

100. WHAT PRODUCT DOES CISCO HAVE THAT WILL ALLOW ENFORCEMENT OF ANTIVIRUS POLICIES ON DESKTOPS (AS WELL AS PATCH POLICIES AND OTHERS)?

The Cisco desktop offering is an intrusion prevention system called Cisco Security Agent. It is managed by a centralized manager called Ciscoworks VPN/Security Management Solution (VMS). It allows for the downloading of custom rules and policies. However, in cases like Blaster, Code Red, Slammer and Nimda, the default policy stops these attacks Day Zero because the default behavior is to stop the type of activity that spreads viruses, such as buffer overflow, writes to the system directly, and writes to the registry.

TO SHARE QUESTIONS, SUGGESTIONS AND OTHER INFORMATION ABOUT NETWORKING SOLUTIONS, PRODUCTS AND TECHNOLOGIES, VISIT THE CISCO FORUM FOR NETWORKING PROFESSIONALS AT WWW.CISCO.COM/GO/NETPRO

Copyright © 2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Cisco IOS, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site 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. (0304R)



THIS IS THE POWER OF THE NETWORK. NOW.