



How to Plan and Implement the Cisco Security Agent on a BBSM Server

Problem Statement

Companies using BBSM may want to protect their Windows-based BBSM server by using the Cisco Security Agent (CSA). Integrating the CSA into another product involves more than just running SETUP.EXE. This whitepaper describes the technical processes required to add protection to the Cisco BBSM product using the CSA. The formal documentation for implementing and using the CSA is available on Cisco Connection Online (CCO) at <http://www.cisco.com>. This whitepaper addresses the necessary steps that you need to get a head start in planning and implementing on the BBSM platform. However, this paper should not be relied upon exclusively to fully implement the CSA on BBSM. This whitepaper only describes the technical efforts to generate a distributable CSA.

Scope

This white paper describes engineering practices, but it does not answer the following product management issues:

- How to coordinate release schedules
- Pricing
- Marketing
- Documentation

Cisco Security Agent Architecture

The architecture of the CSA product (formerly known as *Okena Stormwatch*) contains two active components, which are known as the *Agent* and the *Management Center*. Each protected system runs a copy of the agent, which communicates with, and is controlled by, a Management Center. Agents protect the computer on which they run by interpreting and enforcing *rules* that restrict the operations that the computer can perform. The set of rules being enforced for each computer are called the *security policy*. Security policies are created in the Management Center user interface from building blocks called *policy modules*. Policy modules contain rules and are aggregated into *groups*. Hosts are assigned membership within one or several groups. In summary, a particular host's security policy is the sum of the rules that are contained in the policy modules that are associated with the groups that the host is a member of.

The CSA contains a number of predesigned policy modules. The security policy may be built up from one or several of these predesigned policy modules or from custom-designed policy modules. The Management Center for CSAs is installed as an element of CiscoWorks. The CSAs are installed from kits that are produced using the Management Center.

Tasks

Obtain and License the Software

Contact your Cisco account representative to obtain the CSA software and licenses required to run the product.

Read the Documentation

The best description of the CSA and how to use it is contained in the formal documentation, which ships with the product. This documentation can also be downloaded from the Cisco website: <http://www.cisco.com>. The best advice on how to create a security policy customized for your product is contained in the *Using Management Center for Cisco Security Agents 4.0* document. In particular, the following chapters describe this process in greater detail:

- Building Policies
- Using Cisco Security Agent Profiler
- Policy Definition Guidelines

Understand Your BBSM Product and Your Security Needs

The Security Agent security policies that you create should reflect a well-planned, product-specific security policy. It is important that you spend time charting out your security needs in advance. Study the “Policy Definition Guidelines” chapter, and pay close attention to the list of questions presented early in that chapter. You must have a thorough understanding of the BBSM product before deploying a security policy on the BBSM server. Be careful not to block specific ports that are required for proper BBSM operation. Some of the common ports that BBSM uses are 1433 (SQL), 20 and 21 (FTP), 80 (IIS), 443 (SSL), 50500 (when BBSD is used), 25 (SMTP), and 110 (POP). Other ports may also include the Remote Desktop (RDP) and VNC. Lab testing under an actual usage test is a requirement prior to deployment on production systems.

Consider your security needs. Is your product a locked-down, deeply embedded system? Do you need to provide network or file access to your data sets or to other Cisco or third-party products? Use the Management Center for the CSAs to study the predesigned policy modules. Their design can help you frame your BBSM product’s security needs.

Build the Security Policy

The security policy can be built in several ways. How you build it depends upon factors such as how well you know the BBSM product and how precise your security needs are. There are three ways to create a security policy:

- Use existing predesigned policy modules exclusively.
- Use predesigned policy modules alongside custom-designed policy modules.
- Use the Cisco Security Agent Profiler.

The CSA product documentation describes all of these in detail.

Predesigned Policy Modules

The CSA includes several predesigned policy modules. Some of these modules provide generic support for web servers such as iPlanet, Apache, and Microsoft IIS, DNS, and DHCP servers. By associating one or several of these modules into a single group, you might be able to provide adequate security for your application. For more information about associating policies into a single group, refer to the “Attaching Policies to Groups” section in the “Building Policies” chapter of the *Using Management Center for Cisco Security Agent 4.0* document. By using the predesigned policies, changes can be made to BBSM without fear of having to redeploy the agent for changes to BBSM’s IP and other settings.

Note: The predesigned policies may, however, not be as strict as you want them to be for your particular network deployment.

Crafting New Policy Modules

If you used predesigned policy modules exclusively and you could not create a sufficient security policy to protect your BBSM product, you must create a new policy module. You probably came close just by using the predesigned modules. In that event, you can improve your policy by adding a hand-crafted module to a set of predesigned modules. By using the priority ordering feature to your advantage, you can add individual, narrowly defined rules in your own policy and have them override generic rules in the base policies.

For example, if your application listens on a specific network port, and that action is disallowed by one of the predesigned modules you are using as a base, you can create an “allow” rule that names your specific EXE file and your specific port number. Or, if your application data is stored in a particular directory, you can create a “deny” rule that prevents any other applications from reading from or writing to that directory. You can also have a particular policy per subnet (interface); that is, policies that can differ between the external or internal (AtNatMP) interfaces of BBSM. The CSA can only differentiate between the interfaces by using the subnet range (IP Addresses). If you create a rule that specifies a particular subnet range, if any changes are made to BBSM’s IP structure, a new agent kit must be created and deployed with the appropriate changes.

For a description of the priority ordering feature, see the “Policy Components” section in the “Building Policies” chapter. For instructions for and a methodology of creating security policies, see the “Configuring Policies – The Methodology” section in the “Policy Definitions Guidelines” chapter.

Using Cisco Security Agent Profiler

The Cisco Security Agent Profiler automates the above processes to some degree. You could use the Profiler if you are not sufficiently familiar with the BBSM product, are overwhelmed by the process of creating a policy module manually, or if you want to create a monolithic policy module instead of using the predesigned modules as your base. The “Using Cisco Security Agent Profiler” chapter describes how to use the Profiler. To use the Profiler, install any managed agent on the computer that hosts your application. Then, using the Profiler user interface, select that computer for observation. The Profiler observes the target computer for a period of time that you specify. You should exercise all of BBSM’s features during that time.

At the end of the observation period, the Profiler enters its analysis phase. By examining the behavior of an uncompromised system, the Profiler generates a description of the presumably allowed activity. The Profiler generates a security policy that permits that activity and restricts everything else. The machine-generated security policy is unlikely to be completely satisfactory. It is very important that you study the generated policy and modify it to fit your situation.

Note: The Profiler feature is licensed separately. For the Profiler menu to appear, your Management Center for Cisco Security Agents must be appropriately licensed for this feature.

Study the Result

At this point, whatever method you used, you should have a group with a set of associated policy modules. If you have not done so already, use the *Explain Rules* link on the “Systems -> Groups -> <your group>” page. Study the explanation, share it with your team, and compare it to the security requirements that you previously chose.

Create a Deployable Agent

After you are satisfied with the group’s security policy, but before you can test it, you must create an Agent kit. If you test the security policy in a managed environment, you will gain valuable insight into the operation of your system. In managed mode, all the alerts from all the managed systems are collected into a single, easy-to-use event log in the Management Center. Additionally, for many of the alerts, an associated Event Management Wizard will assist you in modifying your rule set, which is based on information gathered in the Event Log. For more information about the Event Management Wizard, consult the “Event Logging and Alerts” chapter.

The process to test the security policy in a managed environment is described in the “Configuring Groups and Managing Hosts” chapter in the *Using Management Center for Cisco Security Agents 4.0* document. Basically, you must build an agent for your group and install that agent on the test system.

Test the BBSM Product with the Cisco Security Agent

You must test your BBSM product in the presence of the Security Agent that you expect your customers to use. You should conduct the tests that emulate, as closely as possible, the real world usage case to which the agent will be deployed. Testing should include all aspects of client usage such as web browsing, e-mail, file transfers, VPN, and any other possible usage scenario. Other tests should exercise the use of the BBSM management console, both locally and remotely. Make sure to take into account remote access attempts from both allowed and disallowed source IP originations that clients used to make the connection. You should also be prepared to test various security policies by emulating common attacks to see how well your defined rules hold up. You can divide your test to search for two kinds of defects, which are *false positives* and *false negatives*.

A false positive is a defect in which the Security Agent incorrectly identified an innocuous behavior as prohibited. This occurs whenever your product can legitimately be used in a manner not contemplated by the security policy. To exhaustively search for false positives, you must test every distinct feature of BBSM, in every distinct environment that it could run. Depending upon your knowledge of BBSM, you may reduce that effort by eliminating redundant tests.

A false negative is a defect in which an illegitimate action is allowed. There are three types of false negative defects. In the first type, the CSA might not be functioning at all. You can test for this by manually performing some action that you know is disallowed by one or more of your rules. In many security policies you may test for this problem by renaming `c:\winnt\system32\xcopy.exe` to some other name.

A second type of false negative defect occurs when the security policy is insufficiently strict. You must balance your needs to determine exactly how strict your security policy is to be. Refer to the *Using Management Center for Cisco Security Agents 4.0* document for guidance.

A third type of false negative defect is a defect in the CSA technology. This could occur as a result of a bug in the Security Agent or could occur if a new exploit technology is developed. If you suspect defects in the Security Agent technology, contact the TAC for reporting and escalation procedures.

Distribute the Cisco Security Agent to BBSM Servers

You are now ready to distribute the CSA. The agent is in a self-contained, self-installing EXE file. This file can be distributed to your users through any convenient media.



Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0402R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.

Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 6 of 6