

Combating Botnets Using the Cisco ASA Botnet Traffic Filter

This paper discusses the nature of botnets, the threats they pose to today's networks, and how the Cisco[®] Botnet Traffic Filter enables Cisco ASA appliances to fight botnets and to handle their dynamic nature.

Botnet Overview

A botnet is a collection of autonomous software robots (bots), typically malicious in nature, that operate as a network of compromised computers. An originator, also known as a "bot herder," typically controls the bots, and can launch them at will, using command and control communication between the controller and the bots.

Hackers typically use botnets as a way of gaining access to large distributed resources of computing power. The owner of a botnet determines which users are allowed to access their botnet. It is a common practice to even sell access to the botnet.

The following is a typical example of the operation of a botnet:

- A botnet operator will infect computers by sending out viruses or worms through various infection vectors, such as email or compromised websites where the malicious application is the bot.
- The bot on the newly infected host will log into a command and control server and await commands. In many cases, the command and control server will be an IRC channel or a web server.
- A botnet user acquires access to the botnet from the botnet operator.
- Instructions are sent through the command and control channel to each bot in the botnet to execute actions, such as mass email spam, distributed denial of service (DDoS) attacks, or information theft.

This is illustrated in Figure 1.





According to the FBI, in the United States, one to five million hosts are controlled by botnets.¹ The attack profile has evolved from spam and DoS attacks to attacking websites for profit, taking down rival networks, and blackmailing web host owners. There is a significant amount of money at stake. A single DoS attack on a gambling website can cost \$50,000 a day for the business.²

Because the hosts and controllers in a botnet are operating from captured resources, botnets are dynamic and short-lived, which makes them difficult to defeat. As soon as you close down one botnet, it will show up in a different place with new addresses, operating like a network version of a morphing virus.

Botnets have become an important tool in the arsenal of hackers and other criminals that endeavor to profit and to bring financial ruin to companies and individuals with a presence on the Internet.

For further reading on botnets, please refer to the following documents on <u>http://www.cisco.com</u> (<u>http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking_solutions_whitepaper0900a</u> <u>ecd8072a537.html</u>).

Cisco ASA Botnet Traffic Filter

This paper focuses on how Cisco Security Intelligence Operations relates to botnet threat identification, and its interaction with the Cisco ASA Botnet Traffic Filter. It is important to realize that a comprehensive security deployment should include Cisco Intrusion Prevention Systems (IPS) with its reputation based Global Correlation service and IPS signatures in conjunction with the security services provided by the ASA security appliance such as Botnet Traffic Filter.

Cisco Security Intelligence Operations

The Cisco Security Intelligence Operations Center provides customers with the benefits of an industryunprecedented security center, centralizing information and threat signatures issued for all Cisco security technologies, including email filtering, web filtering and reputation, IPS/IDS filtering, and voluntary global threat statistics (Figure 2).

The Cisco Threat Operations Center provides human oversight of Cisco Security Intelligence Operations to ensure speed and accuracy of its threat data, including web and email reputation data, Cisco IPS global correlation data, and botnet database.

Cisco Security Intelligence Operations is the world's largest email and Web traffic monitoring network. With data on more than 25 percent of the world's Internet traffic, it provides an unprecedented real-time view into security threats from around the world. Cisco Security Intelligence Operations can be used like a "credit reporting service" for email and web threats, providing comprehensive data that ISPs and companies can use to differentiate legitimate senders from spammers and other attackers, and giving email administrators visibility into who is sending them email.

¹ FBI initiative, Operation BotRoast. June 2007.

² MSNBC, April 2007, <u>http://redtape.msnbc.com/2007/04/virus_gang_warf.html</u>.





Cisco ASA Botnet Traffic Filter Overview

Cisco ASA 5500 Series Adaptive Security Appliances provide reputation-based control for an IP address or domain name, similar to the control that IronPort[®] SenderBase[®] provides for email and web servers. This has proved to be very successful in combating rogue email and web servers that typically use dynamic or changing IP addresses.

The Cisco ASA Botnet Traffic Filter is integrated into all Cisco ASA appliances, and inspects traffic traversing the appliance to detect rogue traffic in the network. When internal clients are infected with malware and attempt to phone home across the network, the Botnet Traffic Filter alerts the system administrator of this though the regular logging process for manual intervention. This is an effective way to combat botnets and other malware that shares the same phone-home communications pattern.

The Botnet Traffic Filter monitors all ports and performs a real-time lookup in its database of known botnet IP addresses and domain names. Based on this investigation, the Botnet Traffic Filter will determine if a connection attempt is benign and should be allowed, or if it is a risk and should be tagged for mitigation.³

Figure 3 shows how the Botnet Traffic Filter works.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

³ Cisco ASA Software Release 8.2.1 does not support dynamic blocking of this traffic. This will be addressed in a later software release.



Figure 3. Cisco ASA Botnet Traffic Filter Operation

The Cisco ASA Botnet Traffic Filter has three main components:

• Dynamic and Administrator Blacklist Data

The Botnet Traffic Filter uses a database of malicious domain names and IP addresses that is provided by Cisco Security Intelligence Operations. This database is maintained by Cisco Security Intelligence Operations and is downloaded dynamically from an update server. Administrators can also configure their own local blacklists and whitelists.

Traffic Classification and Reporting

Botnet Traffic Filter traffic classification is configured through the dynamic-filter command as shown in Step 3 in the configuration section. The dynamic filter compares the source and destination addresses of traffic against the IP addresses that have been discovered for the various lists available (dynamic black, local white, local black), and logs and reports the hits against these lists accordingly.

Domain Name System (DNS) Snooping

In order to map IP addresses to domain names that are contained in the dynamic database or local lists, the Botnet Traffic Filter uses DNS snooping in conjunction with DNS inspection. Dynamic Filter DNS snooping looks at User Datagram Protocol (UDP) DNS replies and builds a DNS reverse cache (DNSRC), which maps the IP addresses in those replies to the domain names they match. DNS snooping is configured via the Modular Policy Framework (MPF) policies.⁴

⁴ <u>http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/mpc.html</u>

Classification

Traffic that passes through the Botnet Traffic Filter is classified into four categories:

Blacklist

This is traffic to or from an IP address that is considered to be malicious. This IP address can be either an IP address/network entry in the dynamic blacklist or administrator-configured blacklist, or it can be a snooped IP address that was found in a DNS reply for a blacklisted domain.

• Whitelist

This is traffic to or from an IP address that is considered to be good. It is part of the administrator-configured lists.

• Greylist

A greylist IP address has been resolved to one or more blacklist entries as well as one or more unknown entries.

Unknown/None

An IP address that does not map to a domain in either a blacklist or whitelist. No syslogs or statistics will be generated for this traffic.

Once an IP address is found for a blacklisted domain, a rule is added to the dynamic-filter ASP rule table and statistics are kept for the number of times that domain is hit, the client that was accessing it, and the TCP/UDP port that was used to connect. In addition, log messages are produced when a blacklisted IP address is hit that details the src/dst IP and ports as well as the domain name. A similar process is applied for white listed Fully Qualified Domain Names (FQDNs).

Using the Botnet Traffic Filter, Cisco ASA administrators can get statistics for the overall number of blacklist, whitelist, and greylist hits for an interface, as well as summary reports for recent activity.

Dynamic Filter DNS Snooping

The Dynamic Filter DNS snooping feature looks at UDP DNS replies (A and CNAME records only) and builds a DNSRC that maps the IP addresses in those replies to the domain names they match.

DNS snooping should only be enabled for DNS traffic. Failure to do so will result in non-DNS traffic being dropped because it is not adhering to the DNS protocol. DNS snooping should only be enabled for the interface that is facing the Internet, since the Botnet Traffic Filter database is aimed at addressing the external threat of botnets.

It is also not a good practice to fill up your DNSRC with internal information, which can cause early flushing of external information.

DNSRC housekeeping removes entries from the DNSRC on a regular basis.⁵ The amount of time that an entry stays in the DNSRC depends on the time to live (TTL) value in the DNS reply that was snooped.

⁵ The default housekeeping interval is 20 minutes, but is adjusted shorter as the DNSRC grows.

Example of the Botnet Traffic Filter in Action

The client attempts to connect to phone-home server "command-control.badguy.ru."

- 1. Client issues a DNS query for "command-control.badguy.ru."
- 2. The ASA DNS inspection snoops the query and the response to the DNS query and caches it for later use.
- 3. Client connects to IP address of "command-control.badguy.ru."
 - Botnet Traffic Filter resolves IP address in BTF DNS cache.
 - · Botnet Traffic Filter looks up DNS name for connection in Botnet Traffic Filter block list.
 - If peer address is found in Botnet Traffic Filter block list and is not in the manual whitelist, then alert via logging that an illegal connection was attempted.
 - If peer address is not found, then allow connection to continue.

Deployment Guidelines

The Cisco ASA appliance with the Botnet Traffic Filter should be deployed at the edge of the enterprise Internet edge, as the botnet database only contains information about external botnets. It is also best to address the external threat as close to the source as possible. This feature is restricted to IPv4 traffic.

The Botnet Traffic Filter is supported in all firewall modes (single and multiple), and in routed and transparent modes.

The Cisco ASA appliance supports Botnet Traffic Filter in High Availability (HA) mode (Active/Active and Active/Standby). It is essential to note that the DNSRC is not replicated between the ASA HA devices and must therefore be relearned upon a device failover event.

A typical Botnet Traffic Filter deployment will be where the ASA appliance is deployed between the Internet and the corporate networks. The corporate networks in can be divided across multiple interfaces and will, from the Botnet Traffic Filter's point of view, be considered internal networks.

The following steps will need to be taken when configuring Botnet Traffic Filter dynamic filtering:

- 1. Enable DNS client on ASA to allow it to resolve the address of CSIO's updater service, so the dynamic filter update client to fetch updates.
- 2. Enable dynamic traffic filtering (Botnet Traffic Filter).
- 3. Enable the Botnet Traffic Filter database update.
- 4. Classify the traffic that will be subject to dynamic traffic filtering by creating an access control list (ACL) that matches the traffic to be filtered.
- 5. Enable dynamic filtering on the Internet-facing (external) interface by using the classification ACL defined in the previous step.
- 6. Enable DNS snooping on the external interface by adding to or modifying the DNS inspection policy map for the external interface.
- 7. Define local whitelists and/or blacklists if needed.

Configuration

In the following sections we show how the Botnet Traffic Filter is configured with CLI and with the Cisco Adaptive Security Device Manager (ASDM), which is the embedded device manager in Cisco ASA 5500 Series security appliances.

CLI Configuration

Step 1. Enable DNS client⁶ on ASA so the dynamic filter updater client can resolve the address of CSIO.

```
dns domain-lookup outside
dns server-group DefaultDNS
    name-server 10.2.1.1
    domain-name mydomain.cisco.com
```

Step 2. Enable dynamic-filter updater-client

dynamic-filter updater-client enable

Step 3. Enable the use of the database downloaded from the update server dynamic-filter use-database

- Step 4. Classify traffic for dynamic-filter on traffic for all protocols access-list dynamic-filter_acl extended permit ip any any
- Step 5. Enable dynamic-filter classification on outside interface dynamic-filter enable interface outside classify-list dynamic-filter_acl

Step 6. Enable dynamic DNS snooping on outside interface

class-map dynamic-filter_snoop_class match port udp eq domain

policy-map dynamic-filter_snoop_policy
 class dynamic-filter_snoop_class
 inspect dns dynamic-filter-snoop

service-policy dynamic-filter_snoop_policy interface outside

Step 7. Add entries to local blacklists and whitelists

```
dynamic-filter blacklist
   name bad1.example.com
   name bad2.example.com
   address 10.1.1.1 255.255.255.0
dynamic-filter whitelist
   name good.example.com
   name great.example.com
   name awesome.example.com
   address 10.1.1.2 255.255.255.255
```

Cisco ASDM Configuration

The Botnet Traffic Filter is configured in Cisco ASDM through the use of the Botnet Traffic Filter tab (Configuration > Firewall >Botnet Traffic Filter).

Note: It is still necessary to explicitly configure the DNS inspection for your external interface, through the firewall service policy rules.

⁶ We are using an imaginary domain name server as an example. You must enter your own DNS server information here.

Figures 4 and 5 show how to use Cisco ASDM to configure the Botnet Traffic Filter.

Figure 4. Data Download, Traffic Definitions, Exception Lists



Figure 5. Detailed Settings for Dynamic Filtering



Cisco ASDM provides a comprehensive set of reports and dashboards that will give you basic information about the operations of the Botnet Traffic Filter (Figures 6 through 8).

Figure 6.	Top Botnet Sites and Ports	

The state of the s	Back 🔘 Forward 🛛 🦿 Hel	2			CISC
oring > Botnet Traffic Filter > Reports					
rts					
Top bouter sites	TD Address	Botnat Sta	Connections	Mihole	
66.40.9.250 (data.ale	66 40 9 250	data alexa com	515	WINDS	
209.10.2.3 (cd	209.10.2.3	cdn5.tribalfusion	291	Save as PDF	
209.100.1.100	209.100.1.100		159	Clear Report	
64.123.21.11	64.123.21.11		94		
0 44.23.22.11 (ogi.ale	44.23.22.11	cgi.alexa.com	80		
ළි 63.11.34.123 (leplug 📷	63.11.34.123	ieplugin.com	62		
208.11.222.11 (I1.ze	208.11.222.11	l1.zedo.com	61		
209.123.100.3	209.123.100.3		59		
208.111.123.11 (pay-p	208.111.123.11	pay-per-search.com	54		
66.111.2.3 (contex	66.111.2.3	context3.kanood	49		
0 100 200 300 400 Connections	500				
0 100 200 300 400 Connections	500 Botnet Port	Connerti	me	Save as PDF	
0 100 200 300 400 Connections	Botnet Port	Connecti	ons 617	Save as PDF	
0 100 200 300 400 Connections Top Botnet Ports	Botnet Port tcp 1000 tcp 2001	Connecti	ons 617 472	Save as PDF Clear Report	
0 100 200 300 400 Connections tep 1000 tep 2001	500 Botnet Port tcp 1000 tcp 2001 tcp 23	Connect	ons 617 472 22	Save as PDF Clear Report	
0 100 200 300 400 Connections top 1000 top 2001 top 200 top 2001	800 Botnet Port tcp 1000 tcp 2001 tcp 201 tcp 23 tcp 1001	Connect	ons 617 472 22 19	Save as PDF Clear Report	
0 100 200 300 400 Connections Top Botnet Ports	Botnet Port tcp 1000 tcp 2301 tcp 2001 udp 2000	Connect	ons 617 472 22 19 17	Save as PDF Clear Report	
0 100 200 300 400 Connections Top Botnet Ports	Botnet Port tcp 1000 tcp 2001 tcp 2001 udp 2001	Connect	ons 617 472 22 19 17 17	Save as PDF Clear Report	
0 100 200 300 400 Connections top Botnet Ports top 200 top 200	Botnet Port trp 1000 trp 2001 trp 203 trp 1001 udp 2000 udp 2001 trp 8080	Connecti	ons 617 472 22 19 17 17 9	Save as PDF Clear Report	
0 100 200 300 400 Connections tep 1000 tep 2001 tep 2001 tep 2001 tep 2001 tep 2001 tep 2001 tep 8080 tep 8080	Botnet Port tcp 1000 tcp 2001 tcp 2301 tcp 23 tcp 1001 udp 2000 udp 2001 tcp 8080 tcp 800 tcp 80	Connect	ons 617 472 22 19 17 17 3 3	Seve as PDF	
0 100 200 300 400 Connections Top Botnet Ports	Botnet Port tcp 1000 tcp 2301 tcp 23 tcp 1001 udp 2001 tcp 880 tcp 880 tcp 8192	Connect	ons 617 472 22 19 17 17 17 3 3 3 2	Save as PDF Clear Report	
0 100 200 300 400 Connections Top Botnet Ports tep 1000 tep 2001 tep 2001 tep 2001 tep 2001 tep 8000 tep 98192	Botnet Port tcp 1000 tcp 2001 tcp 2001 tcp 2001 udp 2000 udp 2001 tcp 8080 tcp 60 tcp >8192	Connecti	ons 617 472 22 19 17 17 9 3 3 2	Save as PDF Clear Report	
D 100 200 300 400 Connections Top Botnet Ports tep 1000 tep 2001 tep 2001 tep 2001 tep 8000 tep 9000 tep 9000 tep 9000	Botnet Port tcp 1000 tcp 2001 tcp 2001 tcp 2001 udp 2000 udp 2001 tcp 900 tcp 90 tcp 90 tcp 92	Connect	ons 617 472 22 19 17 17 3 3 2	Save as PDF	





e A fandre fanklaner (1970 formal fanklaner)			
affic Overview	Last updated: 11:07:51 AM		10/441110-1/491046
onnection Ratistics			
6	••••••		
5			
•		Top 10 Protected Servers under SYN Attack	Last updated: 11:07:51 AM
		Monitoring Window Size: 0 mins Display: Table	* Detail
1		Rank Server IP:Port Interface Average Current 1	Iotal Source IP(Last Attack Time)
1105 1104	1107 1109 110		
Connections: 1 NAT Mates: 6			
pped Packets Rate			
		No data available to display	
		No data available to display	
		No data evalable to display	
		tio data available to display	
		No data available to display	
		No data available to display	
		No data available to display. Top Boltnet: Traffic Filler Statistics	Last updated: 11:07:51 A
1103 1104 11	05 1100 1107	No data available to display. Top Bohnet Trieffic Eliker Michielss Top Bohnet Trieffic Eliker Michielss	Last updated: 11:07:51 A
1103 1104 11 A.C. Droped 0 Superturn Droped: 0	05 1100 1107	No data available to display Top Bohnet Traillic Filler SLasistics Top Bohnet Sites Top Bohnet Posts Top Bohnet Mosts Based on: Connections	Last opdated: 11/07/51 AS Deplay: Pre 💌
1169 1184 11 ACS Droped: 0 Dropertism Droped: 0 able Scan and SYN Attack Rates	05 1109 1107	Top Status available to display. Top Status 1: Trailine, Inflore Schedubick Top Status 1: Top Status	Last opdated: 11.07.51 A Deplay: Fre X
1103 1104 11 AC Propert 0 Strates Date Son and SYN Attack Rules	05 1100 1107	Top Bother: Traffic filter Statistics Top Bother: Traffic filter Statistics Top Bother: Statistics Board on: Connections Exception	East opdated: 1107/51 AP Doplay: Tre 3
1103 1104 11 A.C. Proped 0 Strateston Prosped: 0 site Scan and SYN Attack Rates	.05 1107	Top Bolives Traffic Fillers Mediates Top Bolives Traffic Fillers Mediates Top Bolives Traffic Fillers Mediates Board on: Convectors Board on: Convectors Board on: Convectors	Last updated: 11.07.51 Ab Esplay: Pro 256 (data.des.com) (560) 17%. 3 (cold abducce) (560) 19%.
1103 1104 11 ACL Dropedt 0 Frepetion Dropedt 0 elde Scan and SM Alfada Rules	05 1109 1107	Top Status available to display. Top Status 1 Traditics Enforce solutionskies Top Status 1 Traditics Enforce solutionskies Top Status 1 Traditics Enforce solutionskies Beard on: Connections Beard on: Connections 0 Status 2	Last updated: 1107/51 AN Doplay: Pro * 20 (data.des.com) (000) 17% 1.10 (data.des.com) (000) 15% 1.10 (data.des.com) (200) 15%
11 00 11 04 11 A CL Cropped: 0 Depending Despection Solar Scon and SYN Alfada Blates	00 1108 1107	Top Bothest Traffic filler Volatibilitie Top Bothest Traffic filler Volatibilitie Based on: Connections	East updated: 11/07/51 AP Deplay: Pro X 200 (data.des.com) (500) 17%. 13 (data.des.com) (500) 17%. 13 (data.des.com) (500) 17%. 13 (data.des.com) (500) 14 (data.des.com) (500)
1100 1104 11 ACL Proped 0 Properties Proped: 0 soble Scan and SYN Attack Rates	.05 1100 1107	Top States available to display: Tray Bodnets TrickTill Filters Mechanisms Tage Bodnet Dates Tage Indirect Motis Tage Indirected Houts Beed on: Connections 000000000000000000000000000000000000	Last updated: 11:07:51 AF Espin: Pr 256 (dds.des.com) (500) 17%; 1.1 (edg.des.com) (90) 9%; 1.21 (edg.des.com) (91) 9%; 1.22 (edg.des.com) (91) 9%; 1.22 (edg.des.com) (91) 9%;
1103 1104 11 ACL Dropedt 0 Freedom Dropedt 0 Biblis Scan and Stril Alfada Rubes	05 1109 1107	Top Status available to display. Top Status [Top Status] Top Status [Status] Sta	East under de 1107/51 AN Engeley: Port 300 (deta-deta-com) (000) 17%, 13 (cold inducion-com) (200) 19%, 130 (cold inducion-com) (200) 19%, 131 (cold inducion-com) (200) 19%, 131 (cold inducion-com) (200 Hz 22.11 (la cold inducion-com) (200 Hz, 22.11 (la cold inducion-com) (200 Hz, 23.11 (la cold i
1103 1104 11 ACL Property 0 Properties Dropped: 0 safet Scan and SYN Attack Rules	05 1100 1107	Top Softwell Traffic Filler & Statistics Top Bothert Traffic Filler & Statistics Top Bothert Siller Top Docent Points Top Docent Points Beed on: Connections 000000000000000000000000000000000000	Last updated: 11/07/51 AV Doplay: Pro 200 (dda.akra.com) (000) 1% 21 (dda.akra.com) (000) 1% 21 (dda.akra.com) (000) 1% 121 (ddp.akra.com) (00) 4% 120 (ddp.akra.com) (00) 4% 120 (ddp.akra.com) (00) 4% 223 11 (dp.apras.com) (00) 4% 223 11 (dp.apras.com) (00) 4%

Figure 8. Integration of Botnet Traffic Filter Statistics into the ASDM Dashboard

Mitigation

Mitigation is a critical step in the botnet detection and prevention process and security incident response cycle. The following steps can be taken to mitigate botnet infections once they have been identified by the Botnet Traffic Filter.

Manual Process

- 1. Security administrator identifies infected hosts reported by BTF dashboard, and on Cisco ASDM or shown in syslog messages (as shown in the example in the next step). Next, a manual remediation process can be taken.
- 2. Block all transient traffic coming to and from infected hosts using "shun" or ACLs on the ASA appliance. An administrator can perform this by the use of Cisco ASDM⁷ or the CLI. Shun is preferred as it is dynamic and non-persistent and will block existing connections without interfering with the static security policy (ACLs).

Example

The following is a sample syslog message generated by the Botnet Traffic Filter when it detects an infected host that matches the Botnet Traffic Filter dynamic filtering database:

```
ASA-4-338002: Dynamic Filter permitted black listed TCP traffic from inside:10.1.1.45/6798 (209.165.201.1/7890) to outside:209.165.202.129/80 (209.165.202.129/80), destination 209.165.202.129 resolved from dynamic list: bad.example.com
```

Here's how the resulting ACL entry would look:

access-list BLOCK_OUT extended deny ip host 10.1.1.45 host 209.165.202.129 access-list BLOCK_OUT extended permit ip any any access-group BLOCK_OUT out interface outside

The above ACL effectively would block all IP traffic sourced from the infected host 10.1.1.45 when going to the botnet command and control server at 209.165.202.129. Specific source or destination port can be blocked for more granular control, as needed.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

⁷ A reverse ACL can be created using the Cisco ASDM real-time log by right-clicking on the syslog messages generated by the Botnet Traffic Filter.

Here's how the corresponding shun command that blocks communication with the same command and control server would look:

shun 209.165.202.129

- Manually identify ingress/access points of the network (e.g., what switchports infected hosts are plugged into). Disable the switchport(s) and notify end users that their PCs are infected. Dispatch IT person to perform a malware/bot cleanup or re-image the infected PC(s) as necessary.
- 4. Bring the disinfected hosts back online once the threats have been remediated.

Conclusion

The Cisco ASA Botnet Traffic Filter is an effective tool that enterprises can use to gain insights into one of today's leading threats. In conjunction with accurate threat data provided by Cisco Security Intelligence Operations and Cisco Global Correlation for IPS, the Botnet Traffic Filter provides an industry-leading solution to combat modern botnet threats in a dynamic environment.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco Stadium/Vision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, IransPath, WebEx, and the WebEx logo 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. (0903R)

Printed in USA

C11-532091-01 06/09