Cisco Smart Care Firewall Configuration Guide

Introduction
This document provides site firewall configuration guidelines and examples for use when the Cisco® Smart Care Service client is installed in the customer network.

Cisco Smart Care Service uses a collector-agnostic approach, supporting multiple techniques for performing network discovery and network inventory of most Cisco hardware currently in operation. Agents are used to deliver these capabilities. Agents can differ in application size, in how they support dynamic updates to features, and in their use of highly customizable logic in the area of asset management inventory. Data is collected according to specifications and a data model predefined by Cisco.

Cisco Smart Care Service assures the export of data via multiple secure industry-standard data transmission mechanisms. The Smart Care Service back end is used as the central repository of the information collected from customer network equipment. The network client and secure server at Cisco enable the secure data transmission of collected device data to the service back end.

The Cisco Smart Care Service hardware or software client automates the collection and analysis of device data. Using best-in-class device discovery and inventory collection methodologies, it extracts information from network devices. This information is then transported back to Cisco over a secure channel (using HTTPS) for in-depth analysis and data scrubbing of the device information, such as serial number, model, and Cisco IOS® Software version. Once the data is evaluated, the service generates a high-quality network summary, which is made available on a web portal for partner or customer viewing, along with detailed reports.

Prerequisites
This document is applicable to partners entitled to sell Cisco Smart Care Service.

Requirements
We recommend that you review the following documents prior to reading this guide:

- Cisco Smart Care Service User Guide
- Cisco Smart Care Service Security Whitepaper

Components Used

- Cisco Smart Care Service client.
  Information mentioned in this document with regard to the Cisco Smart Care Service client is not specific to a particular release or version. We will assume in this document that the Cisco Smart Care Service client is installed in the customer's inside network, behind any firewalls that may exist in the network.
- Firewall configuration examples shown in this document are specific to Cisco PIX® Firewall and Adaptive Security Appliance (ASA) running version 7.0 and later.
- Router configuration examples in this document are not specific to any Cisco IOS Software release, but are based generally on Cisco IOS Software version 12.0 and later.
Firewall Configuration

We recommend installing the Cisco Smart Care Service client behind the firewall for easier access to the different devices in the customer network. Firewall(s) in the customer network may need to be tuned to allow the Cisco Smart Care Service client to access these network devices. Certain types of traffic will need to be allowed from the Cisco Smart Care Service client’s network inside the firewall to the rest of the customer network, as well as from outside the firewall to the inside network where the Cisco Smart Care Service client is installed. This document addresses both situations.

By default, Cisco routers and switches allow IP traffic to pass through. In most networks, internal routers and switches do not have access-list restrictions configured, and therefore, other than enabling Simple Network Management Protocol (SNMP) on the device, no further configuration tweaking is needed for the device to be properly discovered.

Cisco firewalls, on the other hand, by default block any IP traffic attempting to pass from the outside network to the inside network, and therefore, in situations in which devices to be discovered are in a different inside network segment and are separated from the Cisco Smart Care Service client by a firewall, tweaks to the firewall configuration are necessary.

With a proper Network Address Translation (NAT) configured, however, Cisco firewalls will allow IP traffic originating from the inside network to return back to the inside network without specific configuration tweaks.

Cisco Smart Care Service Client’s Outbound Traffic

The following Cisco Smart Care client outbound traffic will need to be allowed:

- **ICMP Echo Requests**
  You need to have Internet Control Message Protocol (ICMP) echo request access to all customer network devices for discovery.
  - For transit firewalls (assuming inside-to-outside traffic), do the following.
    - **Step 1:** Define the access-list entry.
      - If ICMP traffic is not already allowed through the firewall, you will need to at least enable the echo requests:
        access-list <inside_acl_name> permit icmp host <client_address> any echo
      - The `client_address` is likely the actual Cisco Smart Care Service client IP address configured on the client, especially if it is connected directly to the inside network of the firewall. If a NAT is configured, you will need to specify the inside global IP address of the client instead.
    - **Step 2:** Apply the access list on the proper interface (if not already applied):
      access-group <inside_acl_name> in interface <inside_interface_name>
  - For the device to be discovered, do the following.
    - **Step 1:** Define the access-list entry.
      - ICMP will need to be allowed on the customer devices as well. You need to at least enable ICMP echo requests, as shown in the following example:
        access-list <extended_acl_id> permit icmp host <client_address> any echo
      - Here the destination has been specified as any in the access-list entry for all downstream devices and IP addresses.
    - **Step 2:** Apply the access list inbound on the device interface closest to the Cisco Smart Care Service client (if not already applied):
        interface <interface_id>
        ip access-group <extended_acl_id> in
● SNMP GET (UDP/161)

SNMP GET requests are part of the discovery process of Cisco Smart Care Service; therefore, they should be enabled on all applicable devices. In addition, SNMP UDP/161 should be allowed to pass through the intermediate firewall(s).

- For transit firewalls (assuming inside-to-outside traffic), do the following.
  
  **Step 1:** Define the access-list entry:

  ```sh
  access-list <inside_acl_name> permit udp host <client_address> any eq snmp
  ```

  **Step 2:** Apply the access list on the proper interface (if not already applied):

  ```sh
  access-group <inside_acl_name> in interface <inside_interface_name>
  ```

- For the device to be properly discovered, do the following.

  **Step 1:** Define the access-list entry to allow SNMP to access the device and other downstream devices.

  SNMP will need to be allowed and enabled on the customer devices. It is highly recommended that you restrict SNMP access to only allowed hosts (in our case, the Cisco Smart Care Service client), as shown in the following example:

  ```sh
  access-list <extended_acl_id> permit udp host <client_address> any eq snmp
  ```

  Here the destination has been specified as any in the access-list entry for all downstream devices and IP addresses.

  **Step 2:** Apply the access list inbound on the device interface closest to the Cisco Smart Care Service client (if not already applied):

  ```sh
  interface <interface_id>
ip access-group <extended_acl_id> in
  ```

  **Step 3:** Enable a read-only SNMP on the device.

  **Step 3a:** Create a standard access list to allow only authorized hosts to collect information about the device through SNMP. If such an access list is already configured, add the Cisco Smart Care Service client IP address to it as follows:

  ```sh
  access-list <standard_acl_id> standard permit host <CSCS_Client_IP>
  ```

  **Step 3b:** Create a hard-to-guess SNMP community string, and point it to the access list created in step 3a:

  ```sh
  snmp-server community <community-string> ro <standard_acl_id>
  ```

● HTTPS (TCP/443) and HTTP (TCP/80)

The client will need to access tools.cisco.com through the HTTPS protocol for client registration and normal operations. Follow these guidelines if outbound HTTPS access is restricted in the customer network.

- For transit firewalls (assuming inside-to-outside traffic), do the following.

  **Step 1:** Define the access-list entry:

  ```sh
  access-list <inside_acl_name> permit tcp host <client_address> host <tools.cisco.com_ip-address> eq 443
  ```

  **Step 2:** Apply the access list on the proper interface (if not already applied):

  ```sh
  access-group <inside_acl_name> in interface <inside_interface_name>
  ```

- For routers with downstream HTTPS devices, such as Cisco Catalyst® Express or Cisco Unified Communications Manager, or HTTP devices such as Cisco Unity®, do the following.

  **Step 1:** Define the access-list entry to allow HTTP or HTTPS access downstream:

  ```sh
  ! For HTTPS...
  access-list <extended_acl_id> permit tcp host <client_address> host <https-device> eq 443
  ! For HTTP...
  ```
Step 2: Apply the access list on the proper device interface and in the proper direction, depending on the location of the HTTPS device relative to the router:

```
interface <interface_id>
ip access-group <extended_acl_id> <in|out>
```

Step 3: You still need to configure any transit firewall to pass HTTPS/HTTP traffic from the Cisco Smart Care Service client to the HTTPS/HTTP device(s), so that they are properly discovered and inventoried. You can do this in the same manner described in the previous examples.

- **SSH (TCP/22) and Telnet (TCP/23)**
  
  SSH and Telnet are used by the Cisco Smart Care Service client to run inventory and other assessment services on command-line interface (CLI) devices.
  
  - For transit firewalls (assuming inside-to-outside traffic), do the following.

    **Step 1:** Define the access-list entry. You may configure separate entries for each specific SSH/Telnet device in the network or enable the client to have SSH/Telnet access to the entire customer network. The following is a single SSH/Telnet device access-list entry:

    ```
    !For SSH...
    access-list <inside_acl_name> permit tcp host <client_address> host <ssh-device-ip-address> eq 22
    !For Telnet...
    access-list <inside_acl_name> permit tcp host <client_address> host <telnet-device-ip-address> eq 23
    ```

    **Step 2:** Apply the access list on the proper interface (if not already applied):

    ```
    access-group <inside_acl_name> in interface <inside_interface_name>
    ```

  - For routers with downstream SSH/Telnet CLI devices, do the following.

    **Step 1:** Define the access-list entry to allow SSH/Telnet access downstream, in the same way as for a Cisco firewall.

    **Step 2:** Apply the access list on the proper device interface and in the proper direction, depending on the location of the SSH/Telnet device relative to the router:

    ```
    interface <interface_id>
    ip access-group <extended_acl_id> <in|out>
    ```

    **Step 3:** You still need to configure the transit firewall(s) to pass SSH/Telnet traffic from the Cisco Smart Care Service client to the CLI device(s) for proper operation, as shown in the previous examples.

- **DNS UDP/53 and TCP/53**

  The Cisco Smart Care Service client needs to have access to the DNS servers used in the customer network for name resolution. The DNS servers may be located within the customer network or within its service provider network. In either case, the client should be able to send DNS queries to all client-configured DNS servers through the intermediate firewall(s).

  - For transit firewalls (assuming inside-to-outside traffic), do the following.

    **Step 1:** Define the access-list entry:

    ```
    access-list <inside_acl_name> permit udp host <client_address> <dns-server-ip> eq 53
    access-list <inside_acl_name> permit tcp host <client_address> <dns-server-ip> eq 53
    ```

    **Step 2:** Apply the access list on the proper interface (if not already applied):
access-group <inside_acl_name> in interface <inside_interface_name>

- If the DNS server is in the customer network with restricted DNS access, you will need to configure the
  DNS server upstream router to allow DNS queries to pass from the Cisco Smart Care Service client to the
  DNS server, as follows.

  **Step 1:** Define the access-list entry to allow upstream DNS traffic in the same way as for the Cisco firewall
  above.

  **Step 2:** Apply the access list on the proper device interface and in the proper direction, depending on the
  location of the DNS server relative to the router’s interface:

  interface <interface_id>
  ip access-group <extended_acl_id> <in|out>

  **Step 3:** You still need to configure the transit firewall(s) to pass DNS traffic from the Cisco Smart Care
  Service client to the DNS server for proper operations, as shown in the previous examples.

**Cisco Smart Care Service Client’s Inbound Traffic**

The following Cisco Smart Care Service client inbound traffic will need to be allowed.

- **ICMP Echo Replies**
  As discussed earlier, ICMP is used during the discovery process of Cisco Smart Care Service. For the echo
  requests originally sent by the client, active devices will reply back with “echo reply” ICMP packets. Customer
  networks need to allow at least the “echo reply” packets to the client.

  - For transit firewalls (assuming outside-to-inside traffic), do the following.

    Configure an access-list entry for the client and apply it on the proper interface (if not already applied):

    access-list <outside_acl_name> permit icmp any host <client_inside-global-ip> echo-reply
    access-group <outside_acl_name> in interface <outside_interface_name>

- **SSH (TCP/22)**
  If partners wish to remotely manage the Cisco Smart Care Service client, SSH will need to be enabled on the
  client itself and allowed through transit firewalls.

  - For transit firewalls (assuming outside-to-inside traffic), do the following.

    **Step 1:** Configure a static translation for the client if client administration is required from a network outside
    the firewall.

    If NAT is configured on the customer network, you will need to have a static translation on the firewall
    pointing to the client IP address and then allow SSH traffic for the inside global IP address of the client. All
    outside access to the client shall be through the inside global IP address of the client.

    Note that in some multilevel firewall scenarios, multilevel translation may be required.

    ip nat inside source static <client_address> <inside-global-ip>

    **Step 2:** Define the access-list entry. You may configure separate entries for each specific SSH/Telnet
    device in the network or enable the client to have SSH/Telnet access to the entire customer network. The
    following is a single SSH/Telnet device access-list entry:

    access-list <outside_acl_name> permit tcp host <admin_station> host <client_inside-global-ip> eq 22

    **Step 3:** Apply the access list on the proper interface (if not already applied):

    access-group <outside_acl_name> in interface <outside_interface_name>
• Syslog (TCP/514)
  The TCP/514 port is used for Cisco Smart Care Service syslog operation and other monitoring services running on the client.
  ◦ For transit firewalls (assuming outside-to-inside traffic), do the following.
    Step 1: Configure a static translation for the client (if not already configured).
    If NAT is configured on the customer network, you will need to have a static translation on the firewall pointing to the client and then allow syslog packets to the client.
    Please note that in some multilevel firewall scenarios, multilevel translation may be required.
    Customer network devices residing outside the firewall will need to use the inside global IP address of the Cisco Smart Care Service client for successful device monitoring; however, devices behind the firewall and in the same network as the Smart Care Service client will still need to use the client’s inside local IP address (the IP address configured on the client)
    ip nat inside source static <client_address> <inside-global-ip>
    Step 2: Configure an access-list entry for the client and apply it on the proper interface (if not already applied):
    access-list <outside_acl_name> permit tcp any host <client_inside-global-ip> eq 514
    access-group <outside_acl_name> in interface <outside_interface_name>

• DNS UDP/53 and TCP/53
  Inbound DNS ports are needed in case you have delay-jitter-loss (D JL) service enabled for the customer. The ports are used for the communication between the client and the D JL reflector. The following configuration steps will be required only if the D JL reflector is installed in front of a firewall in the customer network.
  ◦ For transit firewalls (assuming outside-to-inside traffic), do the following.
    Step 1: Configure a static translation for the client (if not already configured).
    If NAT is configured on the customer network, you will need to have a static translation on the firewall pointing to the client and then allow DNS UDP/TCP/53 packets to the client.
    Note that in some multilevel firewall scenarios, multilevel translation may be required.
    Also note that the D JL reflector in this case will need to point to the inside global IP address of the Cisco Smart Care Service client for successful D JL operations.
    ip nat inside source static <client_address> <inside-global-ip>
    Step 2: Configure access-list entries for the client and apply the access list on the proper interface (if not already applied):
    access-list <outside_acl_name> permit tcp any host <client_inside-global-ip> eq 53
    access-list <outside_acl_name> permit udp any host <client_inside-global-ip> eq 53
    access-group <outside_acl_name> in interface <outside_interface_name>

Related Information
• ASA/PIX: Handling ICMP Pings and Traceroute
• How to Configure SNMP Community Strings
• NAT Order of Operation
Cisco Confidential.

<table>
<thead>
<tr>
<th>Americas Headquarters</th>
<th>Asia Pacific Headquarters</th>
<th>Europe Headquarters</th>
</tr>
</thead>
</table>

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, CCSP, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Pay and Learn and Cisco Store are service marks; and Access Registrar, Arista, AyreOS, Bringing the Meeting To You, Catalyst, CCDP, CCIE, CCIP, CCNA, CCNP, CCDP, CCVP, Cisco, the Cisco Certified Internet 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, MediaTona, MeetingPlace, MeetingPlace+ Charge, Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PKI, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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.

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