

ASA 8.3 and Later: Set SSH/Telnet/HTTP Connection Timeout using MPF Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Embryonic Timeout](#)

[Troubleshoot](#)

[Related Information](#)

[Introduction](#)

This document provides a sample configuration for Cisco Adaptive Security Appliance (ASA) with version 8.3(1) and later of a timeout that is specific to a particular application such as SSH/Telnet/HTTP, as opposed to one that applies to all applications. This configuration example uses the Modular Policy Framework (MPF) which was introduced in Cisco Adaptive Security Appliance (ASA) version 7.0. Refer to [Using Modular Policy Framework](#) for more information.

In this sample configuration, the Cisco ASA is configured to allow the workstation (10.77.241.129) to Telnet/SSH/HTTP to the remote server (10.1.1.1) behind the router. A separate connection timeout to Telnet/SSH/HTTP traffic is also configured. All other TCP traffic continues to have the normal connection timeout value associated with **timeout conn 1:00:00**.

Refer to [PIX/ASA 7.x and later/FWSM: Set SSH/Telnet/HTTP Connection Timeout using MPF Configuration Example](#) for the same configuration on Cisco ASA with versions 8.2 and earlier.

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

The information in this document is based on Cisco ASA Security Appliance Software version 8.3(1) with Adaptive Security Device Manager (ASDM) 6.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

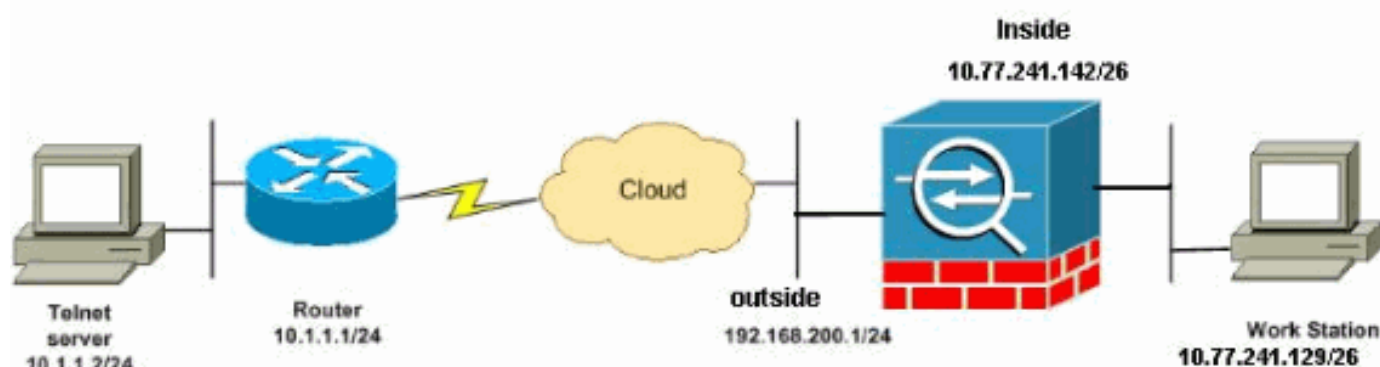
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the [Command Lookup Tool](#) ([registered](#) customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses, which have been used in a lab environment.

Configurations

This document uses these configurations:

- [CLI Configuration](#)
- [ASDM Configuration](#)

Note: These CLI and ASDM configurations are applicable to the Firewall Service Module (FWSM).

CLI Configuration

ASA 8.3(1) Configuration

```
ASA Version 8.3(1)
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 1mZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.0

boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

!--- Creates an object called DM_INLINE_TCP_1. This
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
port-object eq www port-object eq ssh port-object eq
telnet access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover no
asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound access-group 101 in
interface outside route outside 0.0.0.0 0.0.0.0
192.168.200.2 1 timeout xlate 3:00:00 !--- The default
connection timeout value of one hour is applicable to !-
-- all other TCP applications. timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute timeout tcp-proxy-
reassembly 0:01:00 no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh timeout 5 console timeout 0 ! !--- Define the
class map Cisco-class in order !--- to classify
Telnet/ssh/http traffic when you use Modular Policy
Framework !--- to configure a security feature. !---
Assign the parameters to be matched by class map. class-
map Cisco-class match access-list outside_mpc class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
```

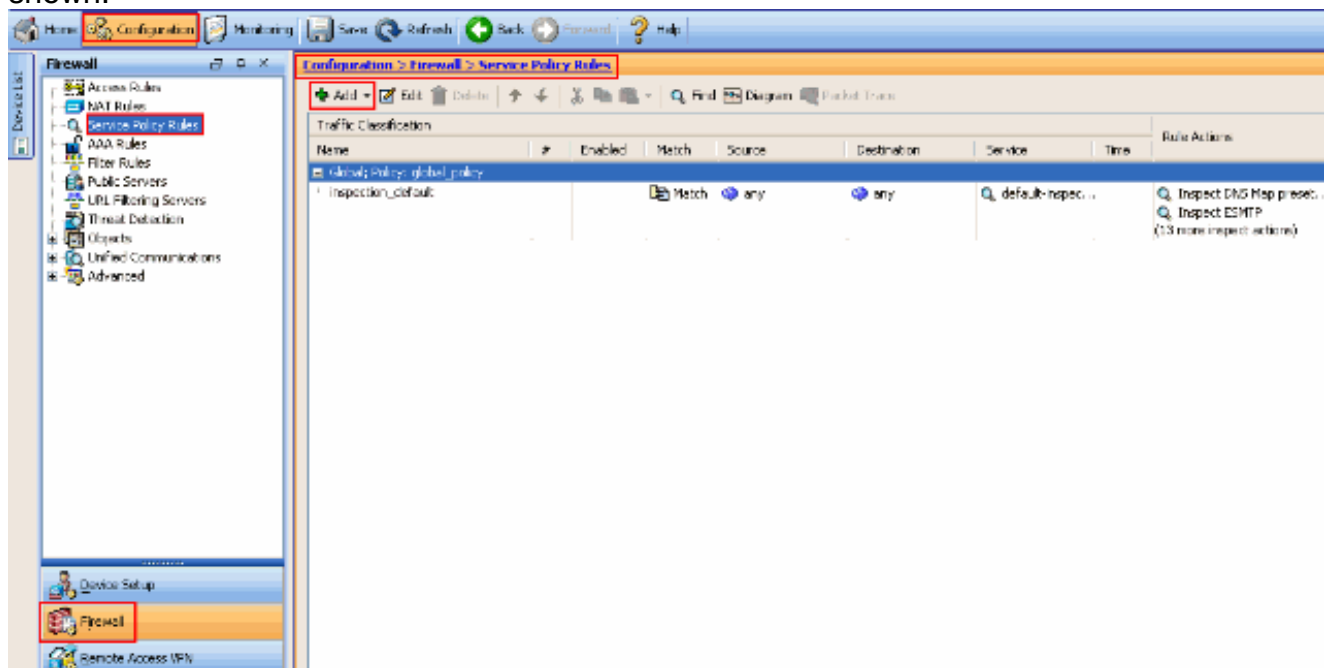
```
inspect sunrpc inspect tftp inspect sip inspect xdmcp !-
-- Use the pre-defined class map Cisco-class in the
policy map. policy-map Cisco-policy !--- Set the
connection timeout under the class mode where !--- the
idle TCP (Telnet/ssh/http) connection is disconnected.
!--- There is a set value of ten minutes in this
example. !--- The minimum possible value is five
minutes. class Cisco-class set connection timeout idle
0:10:00 reset ! ! service-policy global_policy global !-
-- Apply the policy-map Cisco-policy on the interface.
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command. service-policy Cisco-policy interface outside
end
```

ASDM Configuration

Complete these steps in order to set up TCP connection timeout for Telnet, SSH and HTTP traffic using ASDM as shown.

Note: Refer to [Allowing HTTPS Access for ASDM](#) for basic settings in order to access the PIX/ASA through ASDM.

1. Choose **Configuration > Firewall > Service Policy Rules** and click **Add** in order to configure the Service Policy rule as shown.



2. From the **Add Service Policy Rule Wizard - Service Policy** window, choose the radio button next to **Interface** under the **Create a Service Policy and Apply To** section. Now choose the desired interface from the drop-down list and provide a **Policy Name**. The policy name used in this example is **Cisco-policy**. Then, click **Next**.

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

☒ **Interface:** outside - (create new service policy) ▼

Policy Name:

Description:

☐ **Global - applies to all interfaces**

Policy Name:

Description:

< Back **Next >** Cancel Help

3. Create a class map name **Cisco-class** and check the **Source and Destination IP address (uses ACL)** check box in the Traffic Match Criteria. Then, click **Next**.

Add Service Policy Rule Wizard - Traffic Classification Criteria

☒ Create a new traffic class: Cisco-class

Description (optional):

Traffic Match Criteria

- ☐ Default Inspection Traffic
- ☒ Source and Destination IP Address (uses ACL)
- ☐ Tunnel Group
- ☐ TCP or UDP Destination Port
- ☐ RTP Range
- ☐ IP DiffServ CodePoints (DSCP)
- ☐ IP Precedence
- ☐ Any traffic

☐ Use an existing traffic class: inspection_default

☐ Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back Next > Cancel Help

4. From the **Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address** window, choose the radio button next to **Match** and then provide the source and the destination address as shown. Click the drop-down button next to **Service** to choose the required services.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ☒ Match ☐ Do not match

Source: 10.77.241.129

Destination: any

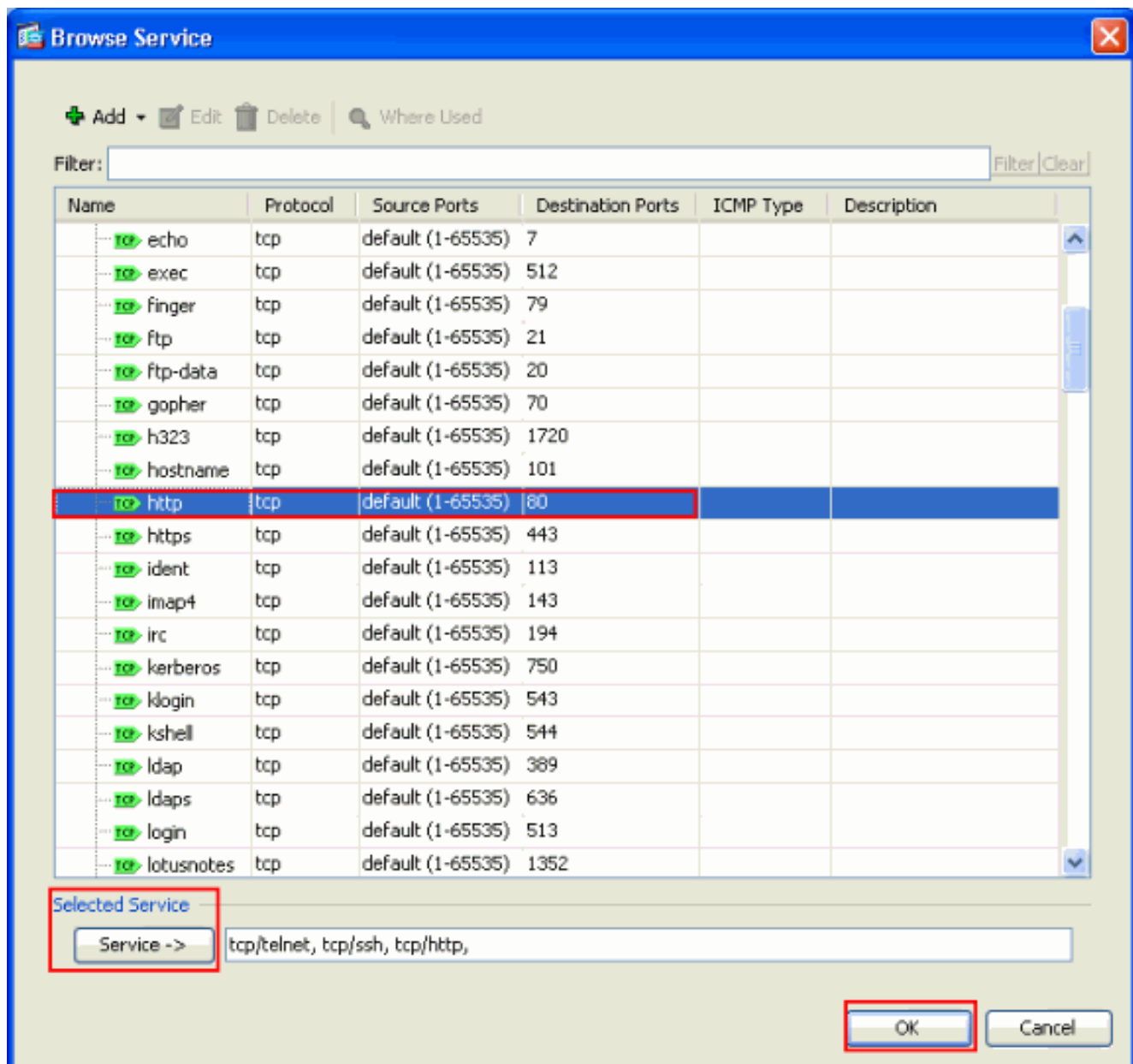
Service: ip

Description:

More Options

< Back Next > Cancel Help

5. Select the required services such as **telnet**, **ssh** and **http**. Then, click **OK**.



6. **Configure Timeouts.** Click **Next.**

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ☒ Match ☐ Do not match

Source: 10.77.241.129

Destination: any

Service: tcp/telnet, tcp/ssh, tcp/http,

Description:

More Options

< Back **Next >** Cancel Help

7. Choose **Connection Settings** in order to set up the TCP Connection Timeout as 10 minutes. Also, check the **Send reset to TCP endpoints before timeout** check box. Click **Finish**.

Add Service Policy Rule Wizard - Rule Actions

Protocol Inspection | Intrusion Prevention | **Connection Settings** | QoS | NetFlow

Maximum Connections

Maximum TCP & UDP Connections: Default (0)

Maximum Embryonic Connections: Default (0)

Maximum Per Client Connections: Default (0)

Maximum Per Client Embryonic Connections: Default (0)

Randomize Sequence Number

Randomize the sequence number of TCP/IP packets. Disable this feature only if another inline ASA is also randomizing sequence numbers and the result is scrambling the data. Disabling this feature may leave systems with weak TCP Sequence number randomization vulnerable.

☒

TCP Timeout

Embryonic Connection Timeout: Default (0:00:30)

Half Closed Connection Timeout: Default (0:10:00)

Connection Timeout: 0:10:00

☒ Send reset to TCP endpoints before timeout

☐ Dead connection detection:

Retries: 5 Timeout: Default (0:15:00)

TCP Normalization

☐ Use TCP map

TCP Map:

Edit... New...

Time to Live

☐ Decrement time to live for a connection

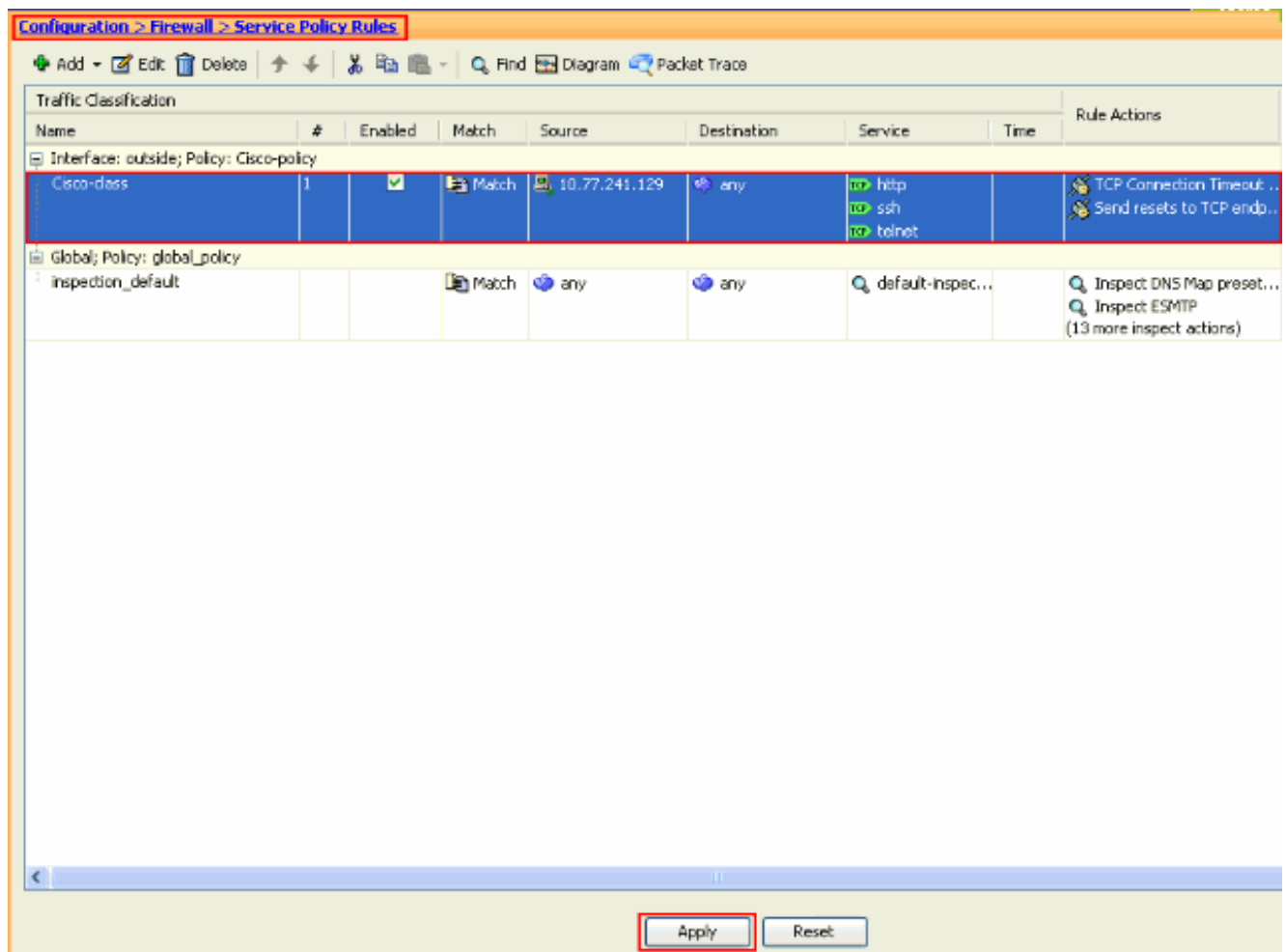
Advanced Options

Skip TCP state tracking and sequence checking when traffic flows across the ASA.

☐ TCP state bypass

< Back Finish Cancel Help

8. Click **Apply** in order to apply the configuration to the Security Appliance. This completes the configuration.



Ebryonic Timeout

An embryonic connection is the connection that is half open or, for example, the three-way handshake has not been completed for it. It is defined as SYN timeout on the ASA. By default, the SYN timeout on the ASA is 30 seconds. This is how to configure Embryonic Timeout:

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map


policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

Troubleshoot

If you find that the connection timeout does not work with the MPF, then check the TCP initiation connection. The issue can be a reversal of the source and destination IP address, or a misconfigured IP address in the access list does not match in the MPF to set the new timeout value or to change the default timeout for the application. Create an access list entry (source and destination) in accordance with the connection initiation in order to set the connection timeout with MPF.

Related Information

- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Requests for Comments \(RFCs\)](#) 
- [Technical Support & Documentation - Cisco Systems](#)