

PIX/ASA 7.X: Disable Default Global Inspection and Enable Non-Default Application Inspection

Document ID: 91891

Introduction

Prerequisites

- Requirements

- Components Used

- Related Products

- Conventions

Default Global Policy

- Disable Default Global Inspection for an Application

- Enable Inspection for Non-Default Application

Related Information

Introduction

This document describes how to remove the default inspection from global policy for an application and how to enable the inspection for a non-default application.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the PIX Security Appliance that runs the 7.x software image.

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.

Related Products

This configuration can also be used with the Adaptive Security Appliance (ASA) that runs the 7.x software image.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Default Global Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can apply only one global policy. If you want to alter the global policy, you must either edit the

default policy or disable it and apply a new one. (An interface policy overrides the global policy.)

The default policy configuration includes these commands:

```
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
service-policy global_policy global
```

Disable Default Global Inspection for an Application

In order to disable global inspection for an application, use the *no* version of the **inspect** command.

For example, in order to remove the global inspection for the FTP application to which the security appliance listens, use the **no inspect ftp** command in class configuration mode.

Class configuration mode is accessible from the policy map configuration mode. In order to remove the configuration, use the *no* form of the command.

```
pixfirewall(config)#policy-map global_policy
pixfirewall(config-pmap)#class inspection_default
pixfirewall(config-pmap-c)#no inspect ftp
```

Note: For more information on FTP inspection, refer to PIX/ASA 7.x: Enable FTP/TFTP Services Configuration Example.

Enable Inspection for Non-Default Application

Enhanced HTTP inspection is disabled by default.

In order to enable HTTP application inspection or in order to change the ports to which the security appliance listens, use the **inspect http** command in class configuration mode.

Class configuration mode is accessible from policy map configuration mode. In order to remove the configuration, use the *no* form of this command.

When used in conjunction with the *http-map* argument, the **inspect http** command protects against specific attacks and other threats that might be associated with HTTP traffic.

For more information on how to use the `http-map` argument with the **inspect http** command, refer to the *inspect http* section of `inspect ctiqbe` through `inspect xdmcp Commands`.

Note: The error message appears as shown when double-encoding is used in some URLs. If you must allow access to this type of website, you can disable the strict HTTP inspection in order to resolve this issue.

```
"%PIX-4-415012:15 HTTP Deobfuscation signature detected - Reset HTTP deobfuscation
detected IDS evasion technique from x.x.x.x to y.y.y.y
```

Note: where `x.x.x.x` and `y.y.y.y` represents the IP addresses

In this example, any HTTP connection (TCP traffic on port 80) that enters the security appliance through any interface is classified for HTTP inspection. *Because the policy is a global policy, inspection occurs only as the traffic enters each interface.*

```
hostname(config)#class-map http_traffic
hostname(config-cmap)#match port tcp eq 80
hostname(config)#policy-map http_traffic_policy
hostname(config-pmap)#class http_traffic
hostname(config-pmap-c)#inspect http
hostname(config)#service-policy http_traffic_policy global
```

In this example, any HTTP connection (TCP traffic on port 80) that enters or exits the security appliance through the *outside interface is classified for HTTP inspection.*

```
hostname(config)#class-map http_traffic
hostname(config-cmap)#match port tcp eq 80
hostname(config)#policy-map http_traffic_policy
hostname(config-pmap)#class http_traffic
hostname(config-pmap-c)#inspect http
hostname(config)#service-policy http_traffic_policy interface outside
```

This example shows how to identify HTTP traffic, define an HTTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)#class-map http-port
hostname(config-cmap)#match port tcp eq 80
hostname(config-cmap)#exit
hostname(config)#http-map inbound_http
hostname(config-http-map)#content-length min 100 max 2000 action reset log
hostname(config-http-map)#content-type-verification match-req-rsp reset log
hostname(config-http-map)#max-header-length request bytes 100 action log reset
hostname(config-http-map)#max-uri-length 100 action reset log
hostname(config-http-map)#exit
hostname(config)#policy-map inbound_policy
hostname(config-pmap)#class http-port
hostname(config-pmap-c)#inspect http inbound_http
hostname(config-pmap-c)#exit
hostname(config-pmap)#exit
hostname(config)#service-policy inbound_policy interface outside
```

Related Information

- [Cisco PIX Firewall Software](#)
- [Requests for Comments \(RFCs\)](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Applying Application Layer Protocol Inspection](#)

- **Cisco Secure PIX Firewall Command References**
 - **Cisco ASA 5500 Series Adaptive Security Appliances**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 10, 2008

Document ID: 91891
