

Configuring the PIX Firewall to Send Authenticated Usernames to a Websense Server

Document ID: 41060

Introduction

Prerequisites

Requirements

Components Used

Conventions

Websense Setup

Cisco Secure ACS Setup

PIX Firewall Setup

What the User Sees

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

The PIX firewall can be configured to communicate with a Websense server to restrict outbound HTTP traffic (FTP and HTTPS in 6.3). The Websense server's essential responsibility is to create and enforce a set of policies to allow or deny access to specific URLs. Websense policies can be assigned at the user level. This affords the Websense Administrator the ability to assign specific access privileges to individual users. The PIX firewall has the capability to send authenticated usernames to the Websense server. This is used to evaluate policy for the specific user. The mechanism by which the PIX firewall sends authenticated usernames to Websense relies upon the PIX having already authenticated the user through the cut-through proxy feature. The PIX functionality of passing authenticated usernames to Websense is only available when the PIX is configured to use the TCP version 4 protocol with Websense.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure PIX Firewall software versions 6.2.2
- Websense Manager, version 4.4.0
- Cisco Secure ACS for Windows version 3.0

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

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Websense Setup

This document assumes that the Websense Administrator has already properly configured the Websense server. It is also assumed here that each user that the PIX is going to authenticate is added as a Directory Object in the Websense Manager, and that this user is configured to be prompted for directory authentication. Consult your Websense documentation or the visit the Websense site for details on how to configure the Websense server.

Cisco Secure ACS Setup

This document assumes that the Cisco Secure ACS Administrator has configured the ACS server to query the same Active Directory/NT database that Websense uses. For information on how to accomplish this task for Cisco Secure ACS for Windows, refer to Working with User Databases.

This document also assumes that the Cisco Secure ACS server has already added the PIX as a client. For details on how to accomplish this task, refer to the AAA Client Configuration section of Setting Up and Managing Network Configuration.

PIX Firewall Setup

These commands are entered on a PIX that already has Internet connectivity

```
!--- Specify AAA server protocols.

aaa-server TACACS protocol tacacs+

!--- This specifies that the authentication server
!--- with the IP address 192.168.253.111 resides on the inside
!--- interface. It is in the default TACACS+ server group.

aaa-server TACACS (inside) host 192.168.253.111 letmein timeout 10

!--- Enable TACACS+ user authentication to the above AAA server.
!--- Users are prompted for authentication credentials.

aaa authentication include http inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 TACACS

!--- Designates server 192.168.253.111 that runs Websense. It is used
!--- in tandem with the filter url command.

url-server (inside) vendor websense host 192.168.253.111 protocol tcp version 4

!--- Enable URL filtering on port 80 (the port that receives Internet traffic).

filter url 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 allow
```

The addition of these commands produces this configuration:

```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

```

nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname TestPIX
domain-name ciscopix.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
pager lines 24
logging on
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 10.0.0.1 255.255.255.0
ip address inside 192.168.253.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip address intf4 127.0.0.1 255.255.255.255
ip address intf5 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address intf4 0.0.0.0
failover ip address intf5 0.0.0.0
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.253.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.0.0.254 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server TACACS protocol tacacs+
aaa-server TACACS (inside) host 192.168.253.111 letmein timeout 10

```

```

url-server (inside) vendor websense host 192.168.253.111 timeout 5 protocol
TCP version 4
aaa authentication telnet console TACACS
aaa authentication include http inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
TACACS
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 allow
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
ssh timeout 5
terminal width 80
Cryptochecksum:d18e45ed25d122af34a5e4f3a183cdf
: end

```

What the User Sees

From a client on the internal network, a browser is opened. Once the browser tries to access an Internet site through the PIX, the user is prompted to enter a username and password. The PIX then sends the username and password to Cisco Secure ACS for Windows to authenticate the outbound HTTP session. Once access is granted by the Cisco Secure ACS server, the PIX sends the authenticated username to the Websense server. The Websense server then looks up the policy associated with the user. It either grants or denies access by sending a response to the PIX. If this response is designed to grant user access, the HTTP transaction between client and server completes. If the response is to deny user access, the PIX drops the HTTP response from the Web server. The browser displays an "access restriction" message.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

