

PIX/ASA: Allow Remote Desktop Protocol Connection through the Security Appliance Configuration Example

Document ID: 77869

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

Related Information

Introduction

This document describes how to allow Remote Desktop Protocol (RDP) connections through a Cisco Security Appliance.

RDP is a multi-channel protocol that allows a user to connect to a computer that runs Microsoft Terminal Services. Clients exist for most versions of Windows, and other operating systems such as Linux, FreeBSD, and Mac OS X. The server listens on TCP port 3389 by default.

In this configuration example, the security appliance is configured to allow an RDP client on the Internet to connect to an RDP server PC on the inside interface. The security appliance performs address translation and the client connects to the host using a static mapped external IP address.

Prerequisites

Requirements

This document assumes that the Cisco PIX Firewall is fully operational and configured. Also, all initial configurations are made and the hosts should have end-to-end connectivity.

Components Used

The information in this document is based on the Cisco PIX 500 Series Security Appliance with software version 7.x.

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

- Cisco Adaptive Security Appliances (ASA) 5500 Series Security Appliance with software version 7.x

Conventions

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

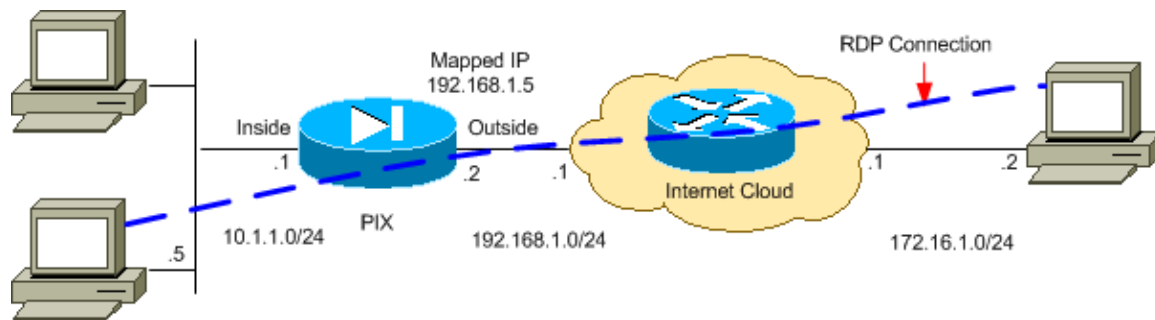
Configure

In this section, you are presented with the information to configure the security appliance to allow the Remote Desktop Protocol (RDP) traffic to pass through.

Note: Use the Command Lookup Tool (registered customers only) 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 section shows the security appliance configuration. RDP traffic from host 172.16.1.2 on the Internet is permitted to host 10.1.1.5 on the inside network which listens on port 3389 through static mapped IP address 192.168.1.5.

Perform these steps:

- Configure static NAT in order to redirect the RDP traffic received on the outside interface to the inside host.
- Create an access control list (ACL) that permits RDP and apply it to the outside interface.

Note: Because NAT is performed by the security appliance, the ACL must permit access to the *mapped* IP address of the RDP server; not the real IP address.

Note: The IP address (192.168.1.5) used for static mapping should be in the same subnet as the outside interface IP address. Refer to the Static NAT section of PIX/ASA 7.x NAT and PAT Statements in order to learn more about static NAT mapping.

PIX

```
pix#show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
access-group 110 in interface outside
!

!--- This access-list allows the RDP traffic sourced from 172.16.1.2
!--- to destination 192.168.1.5 with TCP port 3389.

access-list 110 extended permit tcp host 172.16.1.2 host 192.168.1.5 eq 3389

!--- This staic NAT statement redirects the traffic destined for
!--- IP address 192.168.1.5 to host IP address 10.1.1.5.

static (inside,outside) 192.168.1.5 10.1.1.5 netmask 255.255.255.255
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1

!--- Output is suppressed.
```

Note: In this ACL configuration, "host 172.16.1.2" can be replaced with "any" to allow access to the RDP server from the Internet at large. This is *not recommended*, however, since it might open the RDP server up to attack. As a general rule, make ACL entries as specific as possible.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

- If a certain client or range of clients is unable to connect to the RDP server, be sure that those clients are permitted in the ACL on the outside interface.
- If no clients are able to connect to the RDP server, be sure that an ACL on either the outside or the inside interface is not blocking traffic to or from port 3389.
- If no clients are able to connect to the RDP server, then check to see whether or not the packets exceed the MSS value. If so, configure the MPF to allow the exceeded MSS packets in order to resolve this issue as this example shows:

```
pixfirewall(config)#access-list 110 extended permit
tcp host 172.16.1.2 host 192.168.1.5 eq 3389
```

```
!--- This command is wrapped to a second line due to  
!--- spatial reasons.
```

```
pixfirewall(config)#access-list 110 extended permit  
tcp host 172.16.1.2 host 192.168.1.5 eq 80
```

```
!--- This command is wrapped to a second line due to  
!--- spatial reasons.
```

```
pixfirewall(config)#class-map rdpms  
pixfirewall(config-cmap)#match access-list 110  
pixfirewall(config-cmap)#exit  
pixfirewall(config)#tcp-map mss-map  
pixfirewall(config-tcp-map)#exceed-mss allow  
pixfirewall(config-tcp-map)#exit  
pixfirewall(config)#policy-map rdpms  
pixfirewall(config-pmap)#class rdpms  
pixfirewall(config-pmap-c)#set connection advanced-options mss-map  
pixfirewall(config-pmap-c)#exit  
pixfirewall(config-pmap)#exit  
pixfirewall(config)#service-policy rdpms interface outside
```

Refer to the Solutions to Fragmentation Issues section of PIX/ASA 7.x and IOS: VPN Fragmentation in order to learn about the other methods you can use to resolve the MSS problem.

- The RDP session timeout after the TCP default connection timeout value expired. In order to resolve this issue, increase the timeout as shown here:

```
timeout conn 10:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

This command sets the timeout value to ten hours.

Related Information

- [Cisco PIX 500 Series Security Appliances Support Page](#)
- [PIX/ASA 7.x – NAT/PAT Statements](#)
- [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 24, 2008

Document ID: 77869
