Zone−Based Firewall Troubleshooting

Document ID: 109479

Contents

Introduction

This document contains troubleshooting information for zone−based firewall.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Using VPN with Zone−Based Policy Firewall
- Zone−Based Policy Firewall Design and Application Guide

Components Used

This document is not restricted to specific software and hardware versions.

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 Cisco Technical Tips Conventions for more information on document conventions.

Unable to Pass VPN Traffic

Problem

The issue is that VPN traffic is unable to pass across zone−based firewall.

Solution

Allow the VPN client traffic to be inspected by the zone−based Cisco IOS® firewall.

For example, here are the lines to add on the router's configuration:

```
access−list 103 permit ip 172.16.1.0 0.0.0.255 172.22.10.0 0.0.0.255

class−map type inspect match−all sdm−cls−VPNOutsideToInside−1
  match access−group 103

policy−map type inspect sdm−inspect−all
  class type inspect sdm−cls−VPNOutsideToInside−1
   inspect

zone−pair security sdm−zp−out−in source out−zone destination in−zone
  service−policy type inspect sdm−inspect−all
```

Unable to Pass GRE/PPTP

Problem

The issue is that GRE/PPTP traffic is unable to pass through the zone−based firewall.

Solution

Allow the VPN client traffic to be inspected by the zone−based Cisco IOS firewall.

For example, Here are the lines to add on the router's configuration:

```
agw−7206>enable

gw−7206#conf t
gw−7206(config)#policy−map type inspect outside−to−inside
gw−7206(config−pmap)#no class type inspect outside−to−inside
gw−7206(config−pmap)#no class class−default
gw−7206(config−pmap)#class type inspect outside−to−inside
gw−7206(config−pmap−c)#inspect
%No specific protocol configured in class outside−to−inside for inspection.
All protocols will be inspected
gw−7206(config−pmap−c)#class class−default
gw−7206(config−pmap−c)#drop
gw−7206(config−pmap−c)#exit
gw−7206(config−pmap)#exit
```

Check the configuration :

```
gw−7206#show run policy−map outside−to−inside
policy−map type inspect outside−to−inside
 class type inspect PPTP−Pass−Through−Traffic
  pass
```

```
class type inspect outside-to-inside
 inspect
class class-default
 drop
```

Network Reachability

Problem

After the policy for zone−based firewall is applied in the Cisco IOS router, the networks are not reachable.

Solution

This problem might be the asymmetric routing. Cisco IOS firewall does not work in environments with asymmetric routing. Packets are not guaranteed to return through the same router.

Cisco IOS firewall tracks the state of TCP/UDP sessions. A packet must depart and return from the same router for accurate maintenance of state information.

Unable to Pass DHCP Traffic Through a Zone−Based Firewall

Problem

You are unable to pass DHCP traffic through a zone−based firewall.

Solution

Disable self−zone traffic inspection in order to resolve this issue.

Related Information

- **Technical Support & Documentation − Cisco Systems**
- **AnyConnect on IOS with Zone−Based Firewall (ZBFW)**

Updated: Jan 23, 2009 Document ID: 109479