Zonenbasierte Firewall-Fehlerbehebung

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Fehlerbehebung für zonenbasierte Firewall.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Verwenden von VPN mit zonenbasierter Firewall für Richtlinien
- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

VPN-Datenverkehr kann nicht weitergeleitet werden.

Problem

Das Problem besteht darin, dass der VPN-Datenverkehr nicht über eine zonenbasierte Firewall übertragen werden kann.

Lösung

Lassen Sie zu, dass der VPN-Client-Datenverkehr von der zonenbasierten Cisco IOS® Firewall überprüft wird.

Nachfolgend sind die Zeilen aufgeführt, die zur Konfiguration des Routers hinzugefügt werden müssen:

```
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
```

GRE/PPTP konnte nicht übergeben werden.

Problem

Das Problem besteht darin, dass GRE-/PPTP-Datenverkehr die zonenbasierte Firewall nicht passieren kann.

Lösung

Lassen Sie zu, dass der VPN-Client-Datenverkehr von der zonenbasierten Cisco IOS-Firewall überprüft wird.

Im Folgenden sind die Zeilen aufgeführt, die zur Konfiguration des Routers hinzugefügt werden müssen:

```
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
```

Überprüfen Sie die Konfiguration:

```
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
```

Netzwerkverfügbarkeit

Problem

Nachdem die Richtlinie für zonenbasierte Firewalls im Cisco IOS-Router angewendet wurde, sind die Netzwerke nicht erreichbar.

Lösung

Dieses Problem kann das asymmetrische Routing sein. Die Cisco IOS-Firewall funktioniert nicht in Umgebungen mit asymmetrischem Routing. Es ist nicht garantiert, dass Pakete über denselben Router zurückgesendet werden.

Die Cisco IOS-Firewall verfolgt den Status von TCP-/UDP-Sitzungen. Ein Paket muss vom gleichen Router abweichen und zurückgesendet werden, um die Statusinformationen genau zu verwalten.

DHCP-Datenverkehr kann nicht über eine zonenbasierte Firewall weitergeleitet werden.

Problem

Sie können DHCP-Datenverkehr nicht über eine zonenbasierte Firewall weiterleiten.

Lösung

Deaktivieren Sie die Prüfung des Datenverkehrs in der Kernzone, um dieses Problem zu beheben.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems
- AnyConnect auf IOS mit ZBFW (Zone-Based Firewall)