Verhinderung von ICMP-Jumbo-Frames auf den Managed Switches der Serie SG200/300

Ziel

In diesem Artikel soll erläutert werden, warum die Switches der Serien SG200 und SG300 einige ICMP-Jumbo Frames verhindern und andere Jumbo Frames über den Switch übertragen können. Dieser Artikel zeigt, welche Probleme durch ICMP-Jumbo Frames verursacht werden. Der Artikel erläutert außerdem, was ein Denial of Service (DoS)-Angriff ist und wie er sich auf ICMP-Jumbo-Frames bezieht.

Unterstützte Geräte

SG200
SG300

ICMP-Jumbo-Frames über den Switch

Im Folgenden wird erläutert, was Jumbo Frames sind und warum ICMP-Jumbo Frames auf Switches der Serien SG200 und SG300 nicht zulässig sind.

Jumbo-Frames

Die Gigabit Ethernet-Switches (SG200 und SG300) und Fast Ethernet-Switches (Switches der Serie SF200) unterstützen Jumbo Frames. Bei den **Jumbo Frames** handelt es sich um erweiterte Ethernet-Frames, deren Größe zwischen 1.518 Byte und 9.000 Byte liegt. So erhöhen die Jumbo Frames die Datenübertragungsgeschwindigkeit, indem sie mehr Daten pro Frame übertragen, wodurch der Overhead durch Header verringert wird.

Internet Control Message Protocol (ICMP)

ICMP ist ein Netzwerkschichtprotokoll, das Teil der Internet Protocol Suite ist und ICMP-Nachrichten als Reaktion auf Fehler im IP-Datagramm oder zu Diagnose- oder Routingzwecken generiert. ICMP-Fehler werden immer an die ursprüngliche Quell-IP-Adresse des ursprünglichen Datagramms gemeldet. Obwohl dieses Protokoll sehr wichtig für die korrekte Datenverteilung ist, kann es von böswilligen Benutzern für verschiedene Denial-of-Service (DoS)-Angriffe ausgenutzt werden.

DoS-Angriffe verhindern, dass Netzwerk- und Serverressourcen für legitime Benutzer verfügbar sind oder reagieren. Dies geschieht durch das Überschwemmen von Netzwerken mit falschem Datenverkehr. DoS-Angriffe durch Brute-Force-Angriffe belasten die Server- und Netzwerkbandbreite, da sie den Server mit übermäßigem Datenverkehr überfluten. Im Folgenden werden häufige Arten von DoS-Angriffen mit ICMP aufgeführt.

- ICMP-Ping-Flood-Angriff - Bei einem ICMP-Ping-Flood-Angriff sendet der Angriff eine große Anzahl von Ping-Paketen an das Zielsystem, in der Regel mithilfe des Befehls ping vom Host. Auf diese Weise kann das angegriffene System nicht auf legitimen Datenverkehr reagieren.

- ICMP-Schlumpf-Angriff - Ein ICMP-Schlumpf-Angriff überflutet den Opfercomputer mit gefälschten Ping-Paketen. Hierbei handelt es sich um modifizierte Pakete, die eine gefälschte IP-Adresse des Zielopfers enthalten. Dies führt zu einer Übertragung der Fehlinformationen an alle Hosts im lokalen Netzwerk. Alle diese Hosts antworten mit einer Antwort auf das Zielsystem, die dann mit diesen Antworten gesättigt ist.Wenn es viele Hosts in verwendeten Netzwerken gibt, wird das Opfer effektiv durch eine große Menge an Datenverkehr gefälscht werden.

Hinweis: IP-Spoofing bezieht sich auf ein IP-Paket mit einer gefälschten IP-Quelladresse, um die Informationen des Absenders zu verbergen.

- Ping of Death (Toter Ping): Bei einem Ping-of-Death-Angriff sendet der Angreifer dem Opfer ein ICMP-Echo-Anforderungspaket, das größer ist als die maximale IP-Paketgröße von 65.536 Byte. Da das empfangene ICMP-Echoanforderungspaket größer als die normale IP-Paketgröße ist, muss es fragmentiert werden. Daher kann das Opfer die Pakete nicht neu assemblieren, sodass das Betriebssystem abstürzt oder neu startet.

- ICMP-Nuke-Angriff - Bei diesem Angriffstyp werden Nukes über ein ICMP-Paket mit nicht erreichbaren Zielnachrichten vom Typ 3 an das Opfer gesendet. Das Ergebnis dieses Angriffs ist, dass das Zielsystem die Kommunikation mit vorhandenen Verbindungen unterbricht.

Bei Switches der Serien SG200 und SG300 ermöglicht der Denial-of-Service-Schutz Netzwerkmanagern die Konfiguration der Blockierung bestimmter ICMP-Pakete. Standardmäßig werden einige der ICMP-Jumbo Frames blockiert, da viele Netzwerkangriffe wie DoS ICMP nutzen. Aus Sicherheitsgründen blockieren die Firewalls dieser Switches daher ICMP-Jumbo Frames. Dies führt dazu, dass die erforderliche ICMP-Fragmentierung und die DF-Setnachricht den Sender nicht erreichen. Der Absender erhält somit weder Informationen, um seine Pakete in kleinerer Größe zu versenden, noch eine TCP-Bestätigung, dass seine Pakete erfolgreich waren. Anschließend sendet der Sender den Frame kontinuierlich in der gleichen Größe zurück, erreicht aber nie das Ziel, was zu einem Zustand führt, der als "schwarzes Loch" bezeichnet wird.

Verwenden Sie das Webkonfigurationsprogramm, um Jumbo Frames zu konfigurieren, und wählen Sie **Portverwaltung > Porteinstellungen** und dann **Sicherheit > Denial-of-Service-Schutz > Security Suite-Einstellungen,** um DoS-Schutz zu konfigurieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.