Preventie van ICMP Jumboframes op de SG200/300 Series beheerde Switches

Doel

Het doel van dit artikel is te verklaren waarom SG200 en SG300 reeks switches sommige van ICMP jumboframes verhinderen en andere jumboframes toestaan om over de Switch over te gaan. Dit artikel toont wat sommige problemen toe te schrijven aan Jumboframes ICMP zijn. In het artikel wordt ook uitgelegd wat een Denial of Service (DoS)-aanval is en hoe deze zich verhoudt tot ICMP-jumboframes.

Toepasselijke apparaten

SG200
SG300

ICMP-jumboframes via de Switch

Het volgende verklaart wat jumboframes zijn en waarom ICMP jumboframes niet zijn toegestaan op SG200 en SG300 reeks switches.

Jumboframes

De Gigabit Ethernet-switch (SG200 en SG300 Series) en Fast Ethernet-switch (SF200 Series switches) ondersteunen jumboframes. De **Jumboframes** zijn uitgebreide Ethernet-frames die variëren in grootte van de standaard 1.518 bytes tot 9.000 bytes. Zo verhogen de jumboframes de gegevensoverdrachtsnelheid door meer gegevens per frame te dragen, waardoor de overhead van de headers afneemt.

Internet Control Message Protocol (ICMP)

ICMP is een protocol op de netwerklaag dat deel uitmaakt van de internetprotocolreeks die ICMP-berichten genereert als reactie op fouten in het IP-datagram of voor diagnostische of routeringsdoeleinden. ICMP-fouten worden altijd gemeld aan het oorspronkelijke IP-adres van de bron van het oorspronkelijke datagram. Hoewel dit protocol zeer belangrijk is voor het verzekeren van correcte gegevensdistributie, kan het door kwaadwillige gebruikers voor het uitvoeren van verschillende Denial of Service (DoS) aanvallen worden geëxploiteerd.

DoS-aanvallen maken netwerk- en serverbronnen niet beschikbaar of reageren niet op legitieme gebruikers door netwerken te overspoelen met vals verkeer. DoS-aanvallen door brute kracht verbruiken de server en netwerkbandbreedte door de server te overspoelen met overweldigend verkeer. Het volgende zijn gemeenschappelijke types van aanvallen van Dos die ICMP gebruiken.

·ICMP ping Flood Attack — In een ICMP Ping Flood aanval, de aanval stuurt grote aantallen pingpakketten naar het doelsysteem meestal via het pingcommando van de host. Op deze manier kan het aangevallen systeem niet reageren op legitiem verkeer.

·ICMP Smurf Attack — Een ICMP Smurf Attack overspoelt de slachtoffermachine met

spoofed ping-pakketten. Dit zijn aangepaste pakketten die een spoofed IP-adres van het doelslachtoffer bevatten. Dit veroorzaakt een uitzending van de verkeerde informatie aan alle gastheren in het lokale netwerk. Al deze hosts reageren met een antwoord op het doelsysteem, dat dan verzadigd is met die antwoorden.Als er veel hosts in gebruikte netwerken zijn, zal het slachtoffer effectief worden gespoofd door een grote hoeveelheid verkeer.

Opmerking: IP-spoofing verwijst naar een IP-pakket met een vervalst IP-bronadres, met als doel de informatie van de afzender te verbergen.

·Ping of Death — In een ping of death aanval, stuurt de aanvaller het slachtoffer een ICMP echo verzoekpakket dat groter is dan de maximale IP pakketgrootte van 65.536 bytes. Aangezien het ontvangen pakket met ICMP-echoverzoeken groter is dan de normale IP-pakketgrootte, moet het gefragmenteerd zijn. Hierdoor kan het slachtoffer de pakketten niet opnieuw samenstellen, waardoor het OS crasht of opnieuw opstart.

·ICMP Nuke Attack — Bij dit type aanval worden de atoombommen naar het slachtoffer gestuurd via een ICMP-pakket met onbereikbare doelberichten van het type 3. Het resultaat van deze aanval is dat het doelsysteem communicatie met bestaande verbindingen verbreekt.

In SG200 en SG300 Series switches stelt de Denial of Service Prevention netwerkmanagers in staat om het blokkeren van bepaalde ICMP-pakketten te configureren. Standaard worden sommige ICMP-jumboframes geblokkeerd omdat veel netwerkaanvallen zoals DoS ICMP gebruiken, zodat de firewalls van deze switches ICMP-jumboframes blokkeren voor de beveiliging. Dit resulteert in de noodzakelijke ICMP-fragmentatie en het PDF-bericht dat de afzender niet bereikt. De afzender krijgt dus geen informatie om zijn pakketten op een kleinere grootte te verzenden, noch krijgt het een TCP bevestiging dat zijn pakketten succesvol waren. Vervolgens wordt het frame van dezelfde grootte doorgestuurd door de afzender, maar de bestemming wordt nooit bereikt, wat resulteert in een toestand die bekend staat als een "zwart gat."

Gebruik het hulpprogramma voor webconfiguratie om jumboframes te configureren en kies **Poortbeheer > Poortinstellingen** en kies **Beveiliging > Preventie van ontkenning van service > Instellingen voor Security Suite** om DoS-preventie te configureren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.