ICMP-Paketnachrichten verstehen "unerreichbar - Administrator hat Filter untersagt"

Inhalt

Problem

Kenntnis der Paketinformationen, die an die ICMP-Pakete (Internet Control Message Protocol) "unreachable - admin allowed filter" angehängt sind

Cisco Secure Firewall Threat Defense (FTD) - Erfassungsbeispiel:

<#root>

```
device#

show capture CAPO



106 packets captured

   1: 08:12:45.864243       198.51.100.205.7351 > 192.0.2.2.47668:  udp 111
   2: 08:12:46.400812       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   3: 08:12:46.406320       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

unreachable - admin prohibited filter



   4: 08:12:47.936856       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   5: 08:12:47.943936       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   6: 08:12:49.216739       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   7: 08:12:49.222278       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   8: 08:12:50.096079       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   9: 08:12:50.106363       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2
```

unreachable - admin prohibited filter

Umwelt

Sie ist in folgenden Produkten zu finden:

- FTD
- Adaptive Security Appliance (ASA)

Auflösung

Erläuterungen zu ICMP Typ 3, Code 13 Meldungen

Die ICMP-Meldungen "unreachable - admin allowed filter" entsprechen dem ICMP-Typ 3, Code 13 (Destination Unreachable - Communication Administratively Prohibition). Diese Meldungen weisen darauf hin, dass der Datenverkehr explizit von einer Sicherheitsrichtlinie oder einer Zugriffskontrollliste (ACL) abgelehnt wurde und nicht aufgrund von Netzwerkverbindungsproblemen unerreichbar ist.

Analysieren der Paketerfassungsinformationen

Schritt 1: Identifizieren der Quelle von ICMP-Ablehnungsmeldungen

Überprüfen Sie die Paketerfassung, um festzustellen, welche Geräte die Antworten für ICMP Typ

3, Code 13 generieren. In diesem Fall stammen die Ablehnungsnachrichten von bestimmten IP-Adressen (192.0.2.2).

Schritt 2: Überprüfen der ursprünglichen Paket-Header

Die "ICMP deny"-Nachrichten enthalten Informationen zu den ursprünglich blockierten Paketen. Dazu gehören die ursprünglichen Quell- und Ziel-IP-Adressen, Protokollinformationen und Portnummern, die die administrative Sperre ausgelöst haben.

Schritt 3: Ablehnungsnachrichten mit Datenverkehrsmustern korrelieren

Ordnen Sie die ICMP-Antworten den spezifischen Datenverkehrsflüssen zu, die abgelehnt werden. Beispielsweise wurde der UDP-Datenverkehr an Port 7351 von dem Gerät mit der IP-Adresse 192.0.2.2 in der CAPO-Erfassung abgelehnt.

Einschränkungen der Paketerfassungsanalyse

Beim Arbeiten mit textexportierten Paketerfassungen kann die detaillierte Paketanalyse im Vergleich zu binären pcap-Dateien eingeschränkt werden. Für eine umfassende Analyse stellen binäre Paketerfassungsdateien (pcap-Format) vollständigere Informationen bereit, darunter:

- Vollständige Paket-Header und Payload-Informationen
- Präzise Zeitinformation
- Umfassende Funktionen zur Protokolldekodierung
- Erweiterte Filter- und Analyseoptionen

Ursache

Die Ursache liegt typischerweise in einem der folgenden Szenarien:

- ACLs, die so konfiguriert sind, dass sie bestimmte Datenflüsse verweigern
- Firewall-Regeln blockieren bestimmte Protokolle, Ports oder IP-Adressen

In diesem Beispiel wurde die Nachricht von einer Downstream-ACL verursacht.

Verwandte Inhalte

- https://datatracker.ietf.org/doc/html/rfc792
- https://datatracker.ietf.org/doc/html/rfc1812
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html

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.