ICMPパケットメッセージについて("unreachable - admin prohibited filter")

内容

お問い合わせ内容

Internet Control Message Protocol(ICMP)パケットに添付されている「unreachable - admin prohibited filter」のパケット情報を理解します。

Cisco Secure Firewall Threat Defense(FTD)キャプチャの例：

<#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

環境

これは、次の製品のいずれかで確認できます。

- FTD
- 適応型セキュリティ アプライアンス (ASA)

解決策

ICMPタイプ3、コード13メッセージについて

ICMPの「unreachable - admin prohibited filter」メッセージは、ICMPタイプ3、コード13(Destination Unreachable - Communication Administratively Prohibited)に対応しています。 これらのメッセージは、トラフィックがネットワーク接続の問題により到達不能ではなく、セキュリティポリシーまたはアクセスコントロールリスト(ACL)により明示的に拒否されたことを示します。

パケットキャプチャ情報の分析

ステップ 1：ICMP拒否メッセージの送信元を特定する

パケットキャプチャを確認して、どのデバイスがICMPタイプ3、コード13応答を生成しているか

を特定します。この場合、denyメッセージは特定のIPアドレス(192.0.2.2)から発信されています。

ステップ 2元のパケットヘッダーを調べる

ICMP拒否メッセージには、ブロックされた元のパケットに関する情報が含まれます。これには、元の送信元と宛先のIPアドレス、プロトコル情報、および管理上の禁止をトリガーしたポート番号が含まれます。

ステップ 3denyメッセージとトラフィックパターンの関連付け

拒否される特定のトラフィックフローに対するICMP応答を照合します。たとえば、ポート7351へのUDPトラフィックは、CAPOキャプチャのIPアドレス192.0.2.2のデバイスによって拒否されています。

パケットキャプチャ分析の制限事項

テキストをエクスポートしたパケットキャプチャを処理する場合、詳細なパケットごとの分析はバイナリpcapファイルと比較して制限できます。包括的な分析を行うために、バイナリパケットキャプチャファイル（pcap形式）は、次のような詳細な情報を提供します。

- 完全なパケットヘッダーとペイロード情報
- 正確なタイミング情報
- 完全なプロトコルデコード機能
- 強化されたフィルタリングと分析オプション

原因

通常、根本原因は次のいずれかです。

- 特定のトラフィックフローを拒否するように設定されたACL
- 特定のプロトコル、ポート、またはIPアドレスをブロックするファイアウォール規則

この例では、メッセージの原因はダウンストリームACLです。

関連コンテンツ

- 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。