

レイヤ 4 トラフィック モニタはどのようにトラフィックをブロックしますか。

質問：

レイヤ 4 トラフィック モニタは、ミラーリングされたトラフィックだけを受信する場合、トラフィックをどのようにブロックしますか。

環境：

レイヤ 4 トラフィック モニタ - 不審なトラフィックをブロックするように設定された L4TM

解決策：

Cisco Web Security Appliance (WSA) には、すべてのネットワーク ポート (TCP/UDP 0-65535) にわたって不審なセッションをブロックできるレイヤ 4 トラフィック モニタ (L4TM) サービスが組み込まれています。

これらのセッションをモニタまたはブロックするには、TAP (テスト アクセス ポート) デバイスを使用するか、ネットワーク デバイス上のミラー ポート (Cisco デバイス上の SPAN ポート) を設定して、トラフィックを WSA にリダイレクトする必要があります。L4TM のインラインモードは、現時点ではサポートされていません。

トラフィックが元のセッションからアプライアンスにミラーリング (コピー) されているだけでも、WSA は、依然として、TCP セッションを休止させるか、UDP セッションに関する ICMP の「ホスト到達不能」メッセージを送信することによって、不審なトラフィックをブロックできます。

TCP セッションの場合

WSA L4TM がサーバへのパケットまたはサーバからのパケットを受信し、そのトラフィックがブロック処理の対象であった場合、L4TM は、シナリオに応じて、TCP RST (リセット) データグラムをクライアントまたはサーバに送信します。TCP RST データグラムは、TCP RST フラグが 1 に設定された単なる通常のパケットです。

RST を受信したクライアントまたはサーバは、最初にそれを検証し、次に状態を変更させます。RST を受信したクライアントまたはサーバが LISTEN 状態であった場合は RST が無視されます。RST を受信したクライアントまたはサーバが SYN-RECEIVED 状態であり、以前に LISTEN 状態であった場合は、LISTEN 状態に戻り、それ以外の場合は、接続を中断し、CLOSED 状態になります。RST を受信したクライアントまたはサーバが上記以外の状態であった場合は、接続を中断し、ユーザに通知して、CLOSED 状態になります。

次の 2 つの場合については考慮が必要です (どちらの場合もユーザ/クライアントの前にファイアウォールが存在)。

1 つ目は、不審なパケットがファイアウォールの外側から内部ネットワーク内のクライアント

に送信される場合です。RST がサーバに送信され、この場合、通常は RST を転送しないファイアウォールに到達しますが、ファイアウォールは、RST が実際にクライアントから戻ったと認識するため、セッションを終了します。この場合、RST の送信元 IP は、クライアントのスプーフィングされた IP です。クライアントは、セッションを終了します。

2 つ目は、パケットが内部ネットワーク内のクライアントから外部サーバ (ファイアウォールの外側) に送信される場合です。この場合、RST はクライアントに送信され、RST の送信元 IP はサーバのスプーフィングされた IP です。

UDP セッションの場合

不審なトラフィックが UDP セッションから送信される場合と同様の動作が WSA によって実行されますが、TCP RST を送信する代わりに、L4TM は、ICMP のホスト到達不能メッセージ (ICMP タイプ 3 コード 1) をクライアントまたはサーバに送信します。ただし、この場合は、ホストが到達不能であるためにパケットを送信できないことが ICMP メッセージによって示されるので、IP スプーフィングは発生しません。この場合の送信元 IP は、WSA の IP です。

これらの RST および ICMP パケットは、WSA から、データルーティング テーブルを使用して、M1、P1、または P2 経由 (導入方法によって異なる) で送信されます。