ISEによるリダイレクト時にDHCPアドレスを受信しないCatalyst 9000シリーズエンドポイントのトラブルシューティング

内容

お問い合わせ内容

Cisco Catalyst 9000シリーズスイッチでCisco Identity Services Engine(ISE)からのリダイレクトを使用して認証を有効にすると、有線エンドポイントがDynamic Host Configuration Protocol(DHCP)を介してIPアドレスを取得できないことが断続的に発生します。 同じ設定を使用するCatalyst 9000以外のシリーズスイッチでは、問題は見られません。

環境

- 製品ファミリ：Catalyst 9000シリーズ
- DHCP取得エラーが発生したWindowsコンピュータ
- Catalyst 9000シリーズスイッチ上のリダイレクトアクセスコントロールリスト(ACL)がDHCPトラフィックを明示的に拒否しない

解決策

1. 次のdenyステートメントをリダイレクトACLに追加して、DHCPトラフィックを明示的に処理します。

`deny udp any eq bootps any`（すべてのUDP eqブートアップを拒否する）

`deny udp any any eq bootpc`（デフォルト）

deny udp any eq bootpc any（オプション）

2. ACLを変更した後、以前に障害が発生していたデバイスを再認証し、DHCP経由でIPアドレスを正常に取得できることを確認します。

原因

Catalyst 9000シリーズスイッチは、認証が有効になっている場合、古いスイッチモデルとは異なる方法でパケットを処理します。 Catalyst 9000シリーズスイッチでのパケット処理の順序は、次のとおりです。

1. permit Access Control Entry（ACE；アクセスコントロールエントリ）ルールに一致するパケットは、AAAサーバへのリダイレクションのためにCPUに送信されます。

2. deny ACEルールに一致するパケットは、スイッチ経由で転送されます。

3. permitまたはdenyのどちらのACEルールにも一致しないパケットは、次のダウンロード可能アクセスコントロールリスト(DACL)によって処理され、DACLが存在しない場合、パケットは暗黙のdeny ACLにヒットし、ドロップされます。

この処理方法は、デフォルトでDHCPトラフィックを許可し、リダイレクトACLの前に処理されるデフォルトACLを使用する古いスイッチモデルとは異なります。 Catalyst 9000シリーズモデルでは、これらのデフォルトACLは使用されず、代わりにセッション上で実行されているリダイレクトACLとDACLに完全に依存します。 先行Catalystスイッチ上のクローズドモードセッションのデフォルトACLは次のとおりです。

3750#sh ip access-lists Auth-Default-ACL（デフォルトACL）

拡張IPアクセスリストAuth-Default-ACL

    10 permit udp any range bootps 65347 any range bootpc 65348（22件の一致）

    20 permit udp any any range bootps 65347（12件の一致）

    30 deny ip any any

関連コンテンツ

- 802.1X認証用のデフォルトACL
- シスコのテクニカルサポートとダウンロード

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。