



データベースとディレクトリのプロトコル インспекションの設定

この章では、アプリケーション レイヤ プロトコル インспекションを設定する方法について説明します。インспекション エンジンには、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インспекションを行う必要があります。そのため、インспекション エンジンがスループット全体に影響を与えることがあります。

ASA では、デフォルトでいくつかの一般的なインспекション エンジンがイネーブルになっていますが、ネットワークによっては他のインспекション エンジンをイネーブルにしなければならない場合があります。

この章は、次の項で構成されています。

- 「[ILS インспекション](#)」 (P.12-1)
- 「[SQL*Net インспекション](#)」 (P.12-2)
- 「[Sun RPC インспекション](#)」 (P.12-3)

ILS インспекション

ILS インспекション エンジンには、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して Network Address Translation (NAT; ネットワーク アドレス変換) をサポートします。

ASA は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、Port Address Translation (PAT; ポート アドレス交換) はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0 (NAT なし) を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインспекション エンジンをオフにすることをお勧めします。

ILS サーバが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート (通常は TCP 389) の LDAP サーバにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定の間隔 TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、**timeout** コマンドを使用して調整できます。

ILS/LDAP はクライアント/サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ (ADD、DEL、SEARCH、MODIFY など) が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323 (SETUP および CONNECT メッセージ) によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしていません。

ILS インспекションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インспекションには、次の制限事項があります。

- 参照要求および応答はサポートされない。
- 複数のディレクトリ内のユーザは統合されない。
- 1 人のユーザが複数のディレクトリで複数の ID を持つ場合、NAT はそのユーザを認識できない。



(注)

H.225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインの TCP オプションで指定された間隔が経過すると、TCP 接続は切断されます。デフォルトで、この間隔は 60 分に設定されています。

SQL*Net インспекション

SQL*Net インспекションはデフォルトでイネーブルになっています。

SQL*Net プロトコルは、さまざまなパケット タイプで構成されています。ASA はこれらのパケットを処理して、ASA のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、Structured Query Language (SQL; 構造化照会言語) の IANA ポート割り当てとは一致しません。



(注)

SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインспекションをディセーブルにします。SQL*Net インспекションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

ASA は、すべてのアドレスを変換し、パケットを調べて、SQL*Net バージョン 1 用に開くすべての埋め込みポートを見つけます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp) (DEV=6) (HOST=a.b.c.d) (PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ (Connect、Accept、Refuse、Resend、Marker) は、NAT 対象のアドレスがあるかどうかをスキャンされません。また、インспекションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかをスキャンされます。データ長ゼロの Redirect メッセージが ASA を通過すると、後に続く Data メッセージまたは Redirect メッセージは変換対象であり、ポートはダイナミックに開かれると想定するフラグが、接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インспекション エンジンには、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ (Connect、Accept、Refuse、Resend、Marker、Redirect、Data) とすべてのパケットは、ポートおよびアドレスがあるかどうかをスキャンされます。アドレスが変換され、ポート接続が開かれます。

Sun RPC インспекション

この項では、Sun RPC アプリケーション インспекションについて説明します。この項は、次の内容で構成されています。

- 「Sun RPC インспекションの概要」 (P.12-3)
- 「SUNRPC Server」 (P.12-4)
- 「Add/Edit SUNRPC Service」 (P.12-4)

Sun RPC インспекションの概要

Sun RPC インспекション エンジンには、Sun RPC プロトコルのアプリケーション インспекションをイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバ上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス (通常は rpcbind) に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバに送信します。サーバが応答すると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

Sun RPC インспекションには、次の制限事項が適用されます。

- Sun RPC ペイロード情報の NAT または PAT はサポートされていません。
- Sun RPC インспекションは着信 ACL のみをサポートします。Sun RPC インспекションは発信 ACL はサポートしません。これは、インспекション エンジンでセカンダリ接続でなくダイナミック ACL が使用されるためです。ダイナミック ACL は常に入力方向に追加され、出力方向には追加されません。したがって、このインспекション エンジンでは発信 ACL をサポートしません。ASA に設定されているダイナミック ACL を表示するには、**show asp table classify domain permit** コマンドを使用します。**show asp table classify domain permit** コマンドの詳細については、CLI コンフィギュレーション ガイドを参照してください。

SUNRPC Server

[Configuration] > [Properties] > [SUNRPC Server]

[Configuration] > [Firewall] > [Advanced] > [SUNRPC Server] ペインには、ASA を通過できる SunRPC サービスと、その固有のタイムアウト値がサーバ単位で表示されます。

フィールド

- [Interface] : SunRPC サーバが常駐するインターフェイスを表示します。
- [IP address] : SunRPC サーバの IP アドレスを表示します。
- [Mask] : SunRPC サーバの IP アドレスのサブネット マスクを表示します。
- [Service ID] : ASA を通過することを許可する、SunRPC プログラム番号、またはサービス ID を表示します。
- [Protocol] : SunRPC 転送プロトコル (TCP または UDP) を表示します。
- [Port] : SunRPC プロトコルのポート範囲を表示します。
- [Timeout] : SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を表示します。

Add/Edit SUNRPC Service

[Configuration] > [Properties] > [SUNRPC Server] > [Add/Edit SUNRPC Service]

[Configuration] > [Firewall] > [Advanced] > [SUNRPC Server] > [Add/Edit SUNRPC Service] ダイアログボックスでは、ASA を通過することを許可する SunRPC サービス、およびそれらの固有タイムアウトをサーバ単位で指定できます。

フィールド

- [Interface Name] : SunRPC サーバが常駐するインターフェイスを指定します。
- [Protocol] : SunRPC 転送プロトコル (TCP または UDP) を指定します。
- [IP address] : SunRPC サーバの IP アドレスを指定します。
- [Port] : SunRPC プロトコルのポート範囲を指定します。
- [Mask] : SunRPC サーバの IP アドレスのサブネット マスクを指定します。

- [Timeout] : SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を指定します。形式は、HH:MM:SS です。
- [Service ID] : ASA を通過することを許可する、SunRPC プログラム番号、またはサービス ID を指定します。

