A10 THUNDER SERIES

PROXY リプレースガイド

PROXY SG からの置き換えについて

Document No. D-030-03-0100-01-JP

目次

Document No	Date	Comments
D-030-03-0100-01-JP	2023/01/06	初版

1 概要

1.1 他社製品から A10 THUNDER へのリプレースに際して

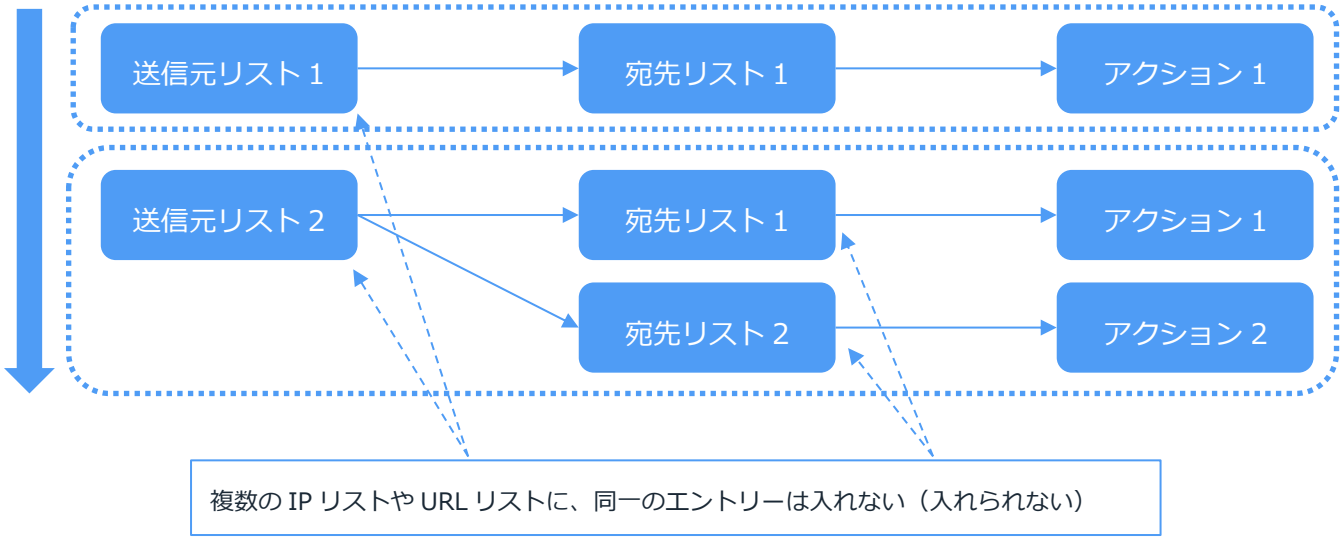
設計思想の異なる他社製品からのリプレースとなる為、単純な機器の入れ替え設定移行作業にはならず、場合によっては一部の機能が移行出来ない、もしくは A10 製品で実装出来る事を基にお客様自身が要件について見直しを行う必要がある事を十分にご理解頂いたうえで、リプレースに進む必要がございます。また、スムーズなリプレースを行う上で事前の動作検証(Proof of Concept)にて求める動作が可能かを予め確認する事を推奨させて頂きます。

1.2 フィルタリングポリシーの動作概要について

以下に各社のフィルタリングポリシーの動作概要について記しております。動作の違いにより、場合によってはフィルタリングポリシーの基になる送信元・宛先リスト等の見直しが必要な場合がございます。

1.2.1 A10 THUNDER のフィルタリングポリシー概要

まず初めに送信元のリストに基づいてマッチング検索を行い、その後それぞれの送信元リストに紐づいた宛先リストのマッチング検索を行う形となっており、全てがユーザー・ユーザーグループ（=送信元リスト）単位で宛先リスト及びアクションのポリシー定義を行う設計思想となっております。

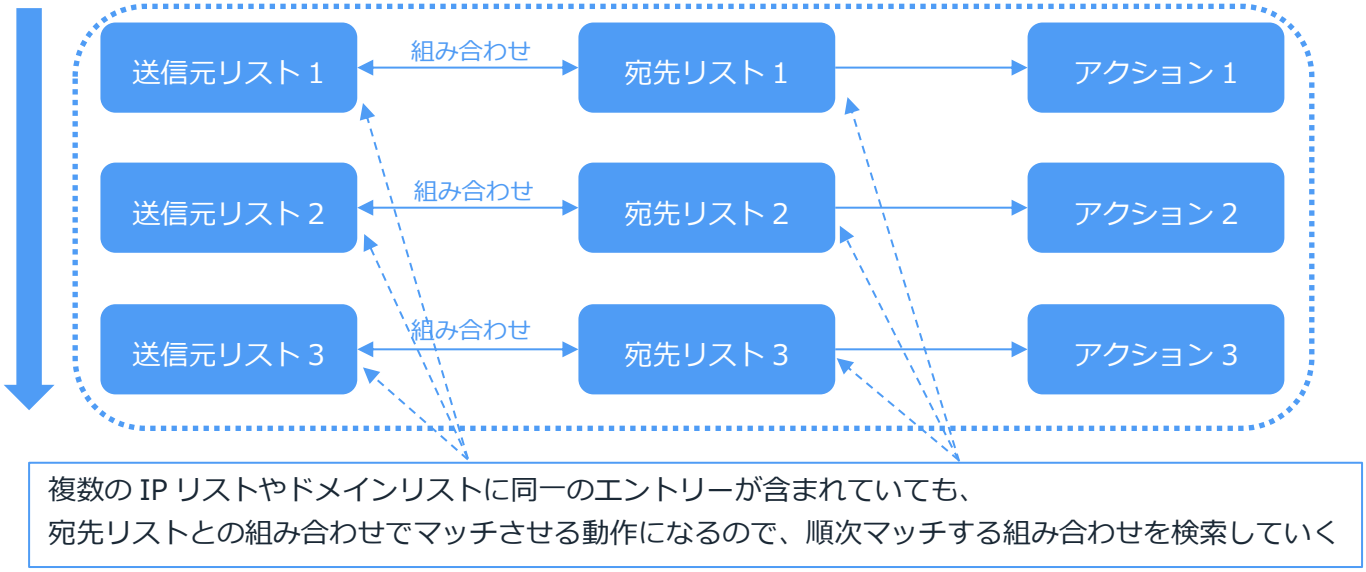


- ユーザー・ユーザーグループ（=送信元リスト）単位で宛先リスト及びアクション等のポリシー定義を行う必要がある
- マッチング高速化による性能向上を図っており、複数のリストで重複したエントリーを予め排除して登録する必要がある

- 複雑な複合条件でのマッチングには対応出来ない場合がある

1.2.2 PROXY SG のポリシーマッチング概要

送信元リストと宛先リストを組み合わせた状態でマッチング検索を行い、マッチするものが見つかるまで順次組み合わせパターンを検索していく設計思想となっている。



- 送信元リスト、宛先リストに重複するエントリーが存在していても動作可能
- マッチングする組み合わせが見つかるまで順次検索するため、一般的に性能が出にくい仕様となる
- 複合的な条件によるマッチング検索が出来る一方、数が多くなると正しい制御が何なのか直感的に把握しづらくなる

1.3 リプレースに際してのチェック項目

機能エリア	項目	確認観点	対応策
送信元・宛先リスト	・送信元 IP リスト ・宛先 IP リスト ・宛先 URL リスト ・Web カテゴリーリスト[1]	・複数のリストにおいて重複した同一エントリーがあるか ・正規表現やワイルドカード文字を使用したマッチングがあるか ・その他、複雑な複合条件によるマッチングがあるか	2.4.1, 3.1 2.4.2, 3.2 3.4 2.6
プロキシアクション	・通信許可 ・通信拒否	・インターネットのサーバーへ直接転送 ・上位プロキシへ転送 ・ドロップ ・特定 URL へリダイレクト[2] ・ブロック画面の表示 [2]	2.5
ユーザー認証・認可	・認証方式 ・認証除外送信元リスト ・認証除外宛先リスト ・LDAP Attribute 参照	・ベーシック認証、Windows 統合認証 ・認証除外リストに多数のエントリーがあるか ・LDAP Attribute による条件分岐、ポリシー制御があるか ・その他、複雑な複合条件によるマッチングがあるか	2.7.1, 2.7.2 3.3 2.7.3 3.4
アクセスログ	・ログ出力内容 ・ログ出力手法	・ログ出力内容やログフォーマットに特別な指定があるか ・TCP・UDP シスログの指定があるか ・複数のシスログサーバーに同一ログを送信するか、負荷分散させるか	2.8, 3.5 2.8.1, 2.8.2 2.8.1, 2.8.2
SSL 可視化	TBD	TBD	TBD
ICAP 連携	TBD	TBD	TBD

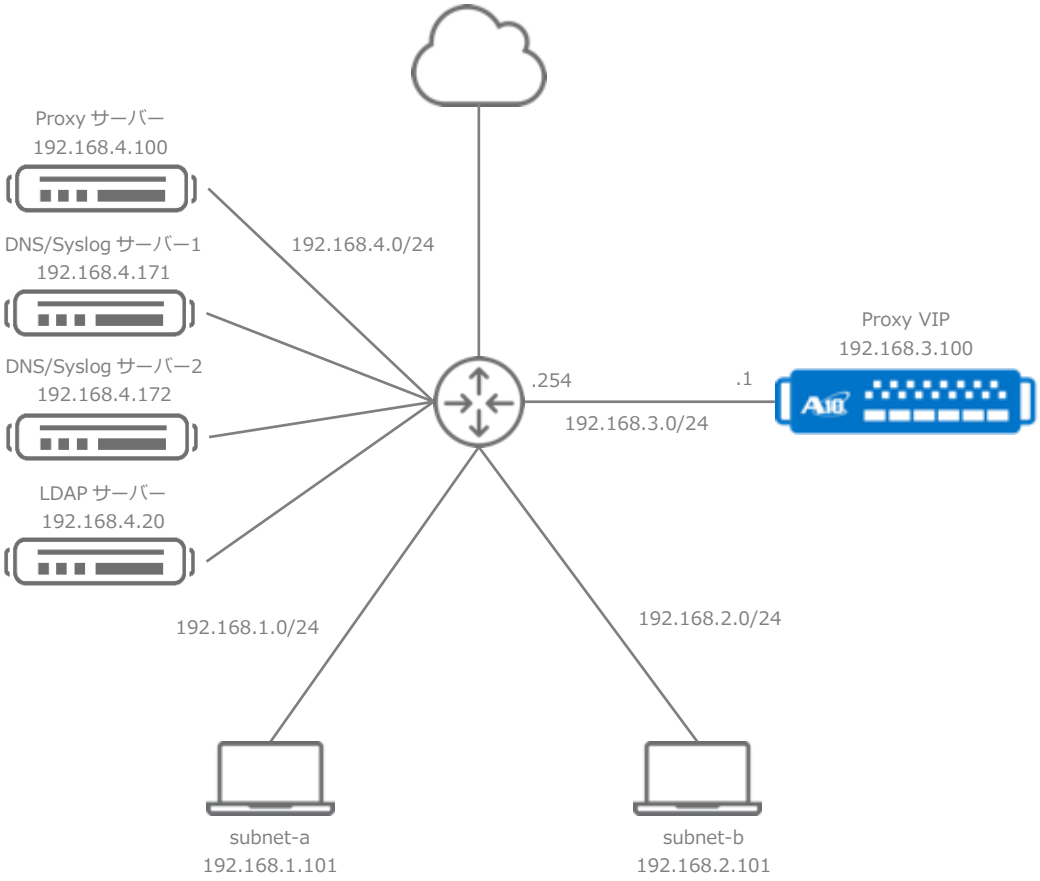
[1] 別途 Bright Cloud のライセンスを購入する必要があります
[2] HTTPS 通信の場合、SSL 可視化機能で復号化する必要があります

2 PROXY サンプル設定

本章では Thunder の典型的な設定例を示します。設定可能な各種パラメータの詳細な内容に関しては割愛している部分もございますので、適宜マニュアル等を併せてご参照ください。

2.1 サンプルネットワーク構成及び概要

以下に簡易ネットワーク構成を示します。



また、ここでは以下の要件としています。

- クライアントは *subnet-a*、*subnet-b* の *2* 種類あり、サブネット毎に *Proxy* のフィルタリングルールを設ける
- ベーシック認証によるユーザー認証を行い、認証サーバーは *LDAP* とする
- 上位に別途 *Proxy* サーバーがあり、上位 *Proxy* サーバーを経由もしくは直接インターネットの 2 通りの接続があり、宛先ドメインによって接続の振り分けを行う
- *DNS*、*Syslog* サーバーはそれぞれ *2* 台あり、*Syslog* に関しては両方のサーバーに同一アクセスログを送信する
- 特定の宛先 *URL* への接続は破棄する