Palo Alto Networks 社製
次世代ファイアウォール
ベンチマークテストレポート

DUT(テスト対象装置: Device Under Test)
Palo Alto Networks PA-3020

2014/05/30

SEC-00003

@benchmark

中規模・大規模企業向け次世代ファイアウォールパフォーマンステストレポート

■ベンチマークテストの内容

アプリケーショントラフィックをテスト対象機器に印加し、テスト対象機器のリソース使用状況をモニタリングする。

■DUT(テスト対象装置: Device Under Test)　Palo Alto Networks 社製 PA-3020

・製品 URL http://www.paloaltonetworks.jp/products/platforms/pa-3000-series.html
・ソフトウェアバージョン:　5.0.11
・アプリケーションバージョン:　425-2146
・脅威バージョン:　425-2146
・アンチウィルスバージョン:　1245-1711
・URL フィルタリングバージョン: 2014.04.02.247

■ベンチマーク使用ポート構成

LAN (Trusted)ポート (1 ポート) 10BASE-T/100BASE-TX/1000BASE-T
WAN (Untrusted)ポート (1 ポート) 10BASE-T/100BASE-TX/1000BASE-T
制御用ポート (1 ポート) 10BASE-T/100BASE-TX/1000BASE-T (SSH 経由)

■テストトラフィックについて

LAN ポートは Trusted ネットワーク、WAN ポートは Untrusted ネットワークとして使用する。各アプリケーションの TCP コネクションは Trusted ネットワーク上の擬似クライアントイニシエートとする。
アプリケーションごとに帯域使用量を変化させ、各帯域使用量での PA-3020 のリソース使用状況を SNMP でモニタリングを行う。

■ベンチマークテスト項目と説明

PA-3020 の PA オプション機能 7 パターンに対し、アプリケーションごとの最大トランザクション毎秒テストとアプリケーションスループットと CPU(MP-CPU, DP-CPU)利用率およびセッション数のリソース使用状況を計測する。 次の項目についてテストを行った。

1.最大トランザクション毎秒テスト

アプリケーションごとの最大トランザクション毎秒テストを行った。アプリケーショントラフィックは、HTTP/HTTPS/FTP/SMTP/DNS とした。

2.アプリケーションスループット性能　x PA-3020A リソース使用状況

アプリケーションスループットを段階的に増加させ、各トラフィック印加時の PA-3020 のリソース使用状況をモニターする。アプリケーショントラフィックは、HTTP/HTTPS/FTP/SMTP とした。

■本資料での専門用語

【フレーム】

ネットワークでデータをやり取りする単位。パケットとほぼ同義語で、レイヤ 2 にかかわる記述ではフレーム、レイヤ 3 にかかわる記述ではパケットと呼ばれる。

【フレームロス】

フレームがスイッチ／ルータ内で処理しきれずに消失すること。

【スループット】

RFC2544[*1] では、測定対象となる装置のフレームロスがない状態でのフレーム最大転送レート。本資料のアプリケーショントラフィックのスループットでは、レイヤ 2 換算でのアプリケーショントラフィック帯域を使用する。

【レイヤ 1 換算のスループット（帯域）】

ネットワーク機器のスループットは 1 秒間の送信フレーム数に各フレームのバイト長 x8 ビットを乗じた値を bps 単位で算出するのが一般的である。フレーム長はレイヤ 2 の Ethernet ヘッダ先頭ビットからレイヤ 2 最後尾の CRC を含んだバイト長で表記されているのが一般だが、物理回線速度の理論上の最大レートは、フレームギャップ(フレーム間隔)96 ビットとプリアンブル(フレームの前につけられるヘッダ情報)64 ビットを含んで算出される。

本資料での「レイヤ 1 換算」とは、スループットの計算に、フレーム長に、フレームサイズ＋プリアンブル＋フレームギャップを使用する。

【レイヤ 2 換算のスループット（帯域）】

ネットワーク機器のスループットは 1 秒間の送信フレーム数に各フレームのバイト長 x8 ビットを乗じた値を bps 単位で算出するのが一般的である。フレーム長はレイヤ 2 の Ethernet ヘッダ先頭ビットからレイヤ 2 最後尾の CRC を含んだバイト長で表記されているのが一般である。

本資料での「レイヤ 2 換算」とは、スループットの計算に、フレーム長に、CRC を含まないバイト長を使用し算出する。

【TCP 新規セッション】

スリーウェイハンドシェイクで開始される、新規の TCP コネクションとする。

【CPS】

毎秒のコネクション数(セッション数)。

【トランザクション】

本資料でのトランザクションとは、擬似クライアントから生成されるアプリケーションコマンドとする。1 つのアプリケーションコマンドで必要な TCP のコネクション数により、トランザクションあたりの TCP コネクション数が異なる。HTTP1.1 persistence 機能では、1 つの TCP コネクション上で、複数トランザクション(HTTP リクエスト)を実現している。

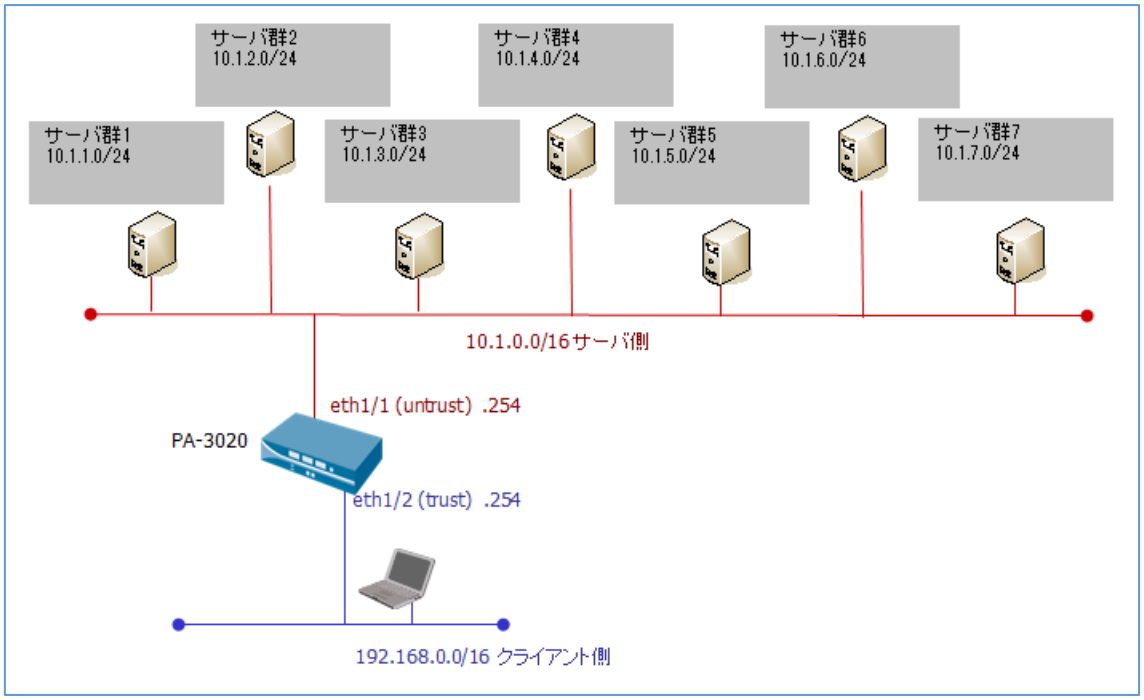
【TPS】

毎秒のトランザクション数。

1.最大トランザクション毎秒テスト

アプリケーション(HTTP/HTTPS/SMTP/FTP/DNS)ごとのトランザクション処理能力を計測する。
各アプリケーションで使用するオブジェクトは以下のテストパラメータに記載する。テストパラメータのHTTP(TXT)、HTTP(ZIP)の表記のように、HTTP GET リクエストに対してのレスポンスのコンテンツとして、テキストファイル(TXT)と ZIP 圧縮ファイル(ZIP)の 2 種類を使用した。
PA-3020 をファイアウォール(UTM)とし、擬似クライアント(Trusted ネットワーク)から擬似サーバ(Untrusted ネットワーク)にアプリケーショントランザクションを発生させる。
PA-3020 のセキュリティ機能(PA オプション機能)は、 アンチウィルス(AV)機能、URL フィルタリング(URL)機能、不正侵入検知システム(IPS)機能、スパイウェア(SPYWARE)機能から、それぞれの機能の単独または組み合わることにより、7 パターンのセキュリティ機能(PA オプション機能)で評価する。
セキュリティ機能(PA オプション機能)は以下のセキュリティポリシーに記載する。
PA-3020 のセキュリティポリシーとして、擬似クライアントがアクセスする擬似サーバの IP アドレスのサブネットの違いによりセキュリティポリシー(PA オプション機能)を設定する。
以下のテスト構成のように、各サーバ群のサブネット上にアプリケーションサーバを擬似する。PA-3020 の設定は、セキュリティポリシー(PA オプション機能)を各サーバ群のサブネット別に設定している。

テスト構成



セキュリティポリシー(PA オプション機能)

セキュリティパターン	PA オプション機能	擬似サーバのサブネット
パターン 1	なし	サーバ群 1
パターン 2	AV	サーバ群 2
パターン 3	URL	サーバ群 3
パターン 4	IPS	サーバ群 4
パターン 5	AV & URL	サーバ群 5
パターン 6	AV& URL & IPS	サーバ群 6
パターン 7	AV & URL & IPS & SPYWARE	サーバ群 7

テストパラメータ

アプリケーション	HTTP/HTTPS/FTP/SMTP/DNS
TCP コネクションごとのトランザクション数	1 トランザクション / 1 コネクション
HTTP(TXT)レスポンスオブジェクト	拡張子 .txt 14 バイト
HTTP(ZIP)レスポンスオブジェクト	拡張子 .zip 148 バイト
HTTPS(ZIP)レスポンスオブジェクト	拡張子 .zip 148 バイト
FTP ファイルサイズ	拡張子 .txt 14 バイト
SMTP メールサイズ	メッセージ:500 バイト 添付: 拡張子 .zip 148 バイト
DNS	レコード数 1 (A レコード)

TCP パラメータ

MSS	1460 バイト
Receive Window	32768 バイト
ポートレンジ	1024 – 65535
再送タイムアウト初期値	300 ミリ秒
最大再送回数	5 回
クローズ方式	クライアント RST

UDP(DNS)パラメータ

ポートレンジ	1024 – 65535
再送タイムアウト初期値	3 秒
最大再送回数	3 回

1-1.テスト結果 (HTTP テキストコンテンツ、HTTP ZIP 圧縮ファイルコンテンツ)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。
非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

1-2.テスト結果 (HTTPS, SMTP, FTP)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。
非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

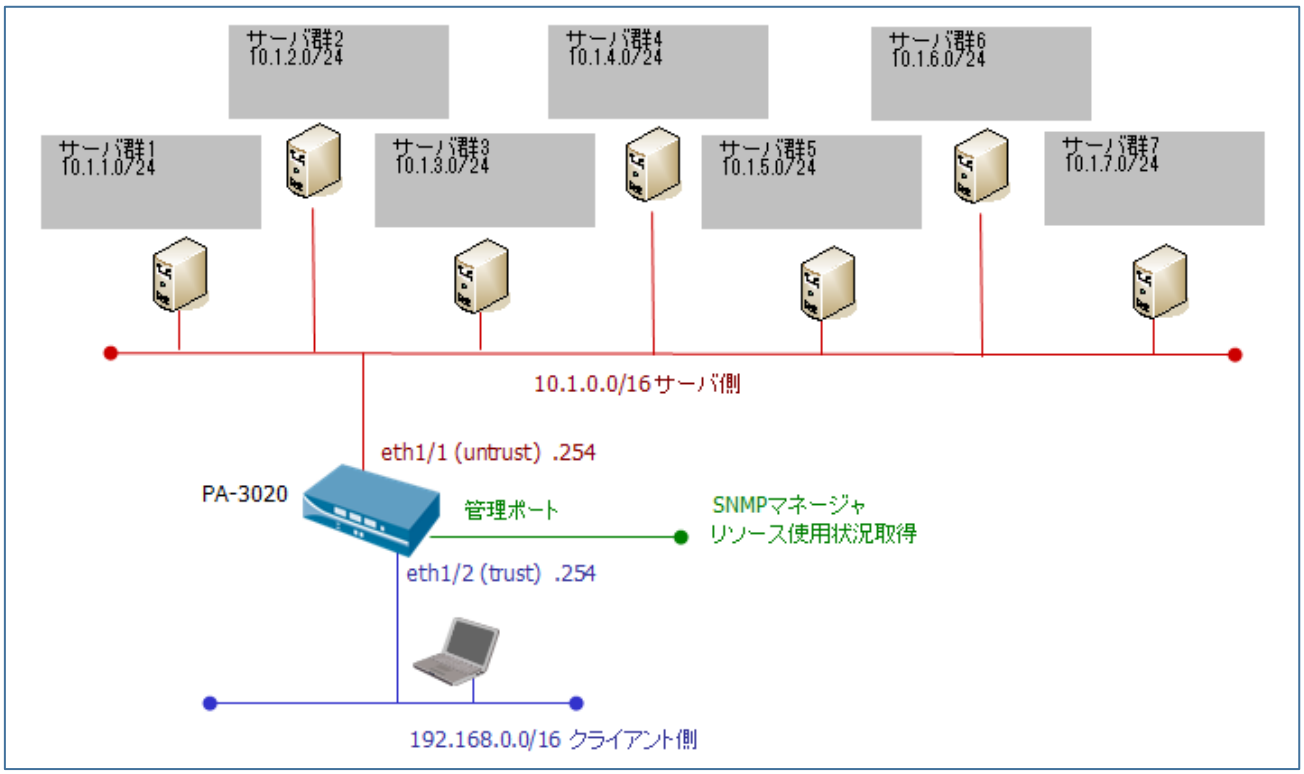
1-3. テスト結果 (DNS)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。
非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

2.アプリケーションスループット性能 x PA-3020A リソース使用状況

PA-3020 をファイアウォール(UTM)とし、擬似クライアント(Trusted ネットワーク)から擬似サーバ(Untrusted ネットワーク)にアプリケーショントランザクションを発生させる。
各アプリケーションでは、1 トランザクション当たりの帯域使用量を増加させるため、コンテンツに 63.5KB の ZIP 圧縮ファイルを使用した。
アプリケーションスループットを段階的に増加させ、各トラフィック印加時に SNMP マネージャを使用し、定期的に PA-3020 から MIB 情報を取得しリソース使用状況をモニターする。テストトラフィックで使用するアプリケーションプロトコルは、HTTP/HTTPS/FTP/SMTP とした。
PA-3020 のセキュリティ機能(PA オプション機能)は、 アンチウィルス(AV)機能、URL フィルタリング(URL)機能、不正侵入検知システム(IPS)機能、スパイウェア(SPYWARE)機能から、それぞれの機能の単独または組み合わせにより、7 パターンのセキュリティ機能(PA オプション機能)で評価する。
以下のテスト構成のように、各サーバ群のサブネットにアプリケーションサーバを擬似する。セキュリティポリシー(PA オプション機能)は各サーバ群のサブネット別に設定している。

テスト構成



セキュリティポリシー(PA オプション機能)

セキュリティパターン	PA オプション機能	擬似サーバのサブネット
パターン 1	なし	サーバ群 1
パターン 2	AV	サーバ群 2
パターン 3	URL	サーバ群 3
パターン 4	IPS	サーバ群 4
パターン 5	AV & URL	サーバ群 5
パターン 6	AV& URL & IPS	サーバ群 6
パターン 7	AV & URL & IPS & SPYWARE	サーバ群 7

テストパラメータ

アプリケーション	HTTP/HTTPS/FTP/SMTP
TCP コネクションごとのトランザクション数	1 トランザクション / 1 コネクション
HTTP(ZIP)レスポンスオブジェクト	拡張子 .zip 63.5K バイト
HTTPS(ZIP)	拡張子 .zip 63.5K バイト

FTP ファイルサイズ	拡張子 .zip　63.5K バイト
SMTP メールサイズ	メッセージ:500 バイト 添付: 拡張子 .zip　63.5K バイト

TCP パラメータ

MSS	1460 バイト
Receive Window	32768 バイト
ポートレンジ	1024 – 65535
再送タイムアウト初期値	300 ミリ秒
最大再送回数	5 回
クローズ方式	クライアント RST

MIB 情報取得の SNMP OID

SNMP ポーリング間隔	5 秒間
MP(Management Plane) CPU	1.3.6.1.2.1.25.3.3.1.2.1
DP(Data Plane) CPU	1.3.6.1.2.1.25.3.3.1.2.2
アクティブセッション数	1.3.6.1.4.1.25461.2.1.2.3.3.0

2-1.テスト結果 (HTTP)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。
非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

2-2.テスト結果 (HTTPS)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。
非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

2-3.テスト結果 (FTP)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。
非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

2-4.テスト結果 (SMTP)

会員の皆さまは会員サイトでログイン後、テストレポートを全てご覧いただけます。

非会員の皆さまは会員申込み（有料）いただければ、本テストレポートの続きをご覧いただけます。

■ベンチマークテスト機材

本ベンチマークテストには下記の測定器を用いた。

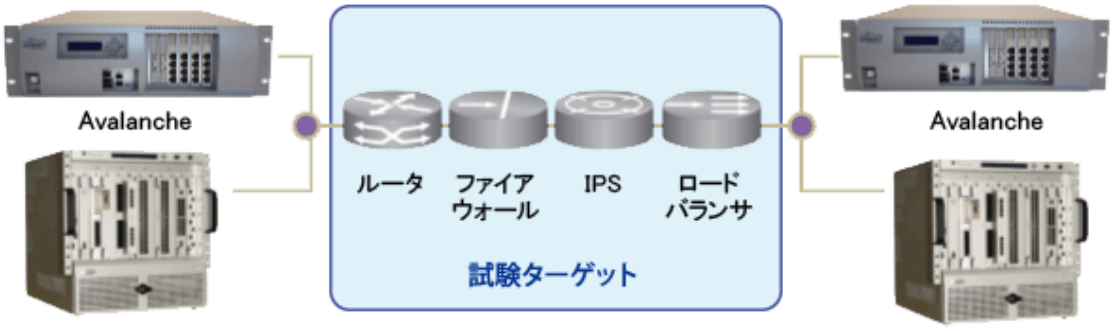
●Spirent Communications 社アプリケーション・パフォーマンス/セキュリティ 試験ツール
Spirent Avalanche Version 4.37

●Spirent Communications 社テスト自動化支援ツール
Spirent iTest Version 4.3.1

●Palo Alto Networks 社製 PA-3020

●Spirent iTest

●Avalanche C100



■リファレンス

*1 http://tools.ietf.org/html/rfc2544
ネットワーク装置のベンチマーク手法
Benchmarking Methodology for Network Interconnect Devices
*2 http://tools.ietf.org/html/rfc3511
ファイアウォール パフォーマンス評価手法
Benchmarking Methodology for Firewall Performance

■PA-3020 設定