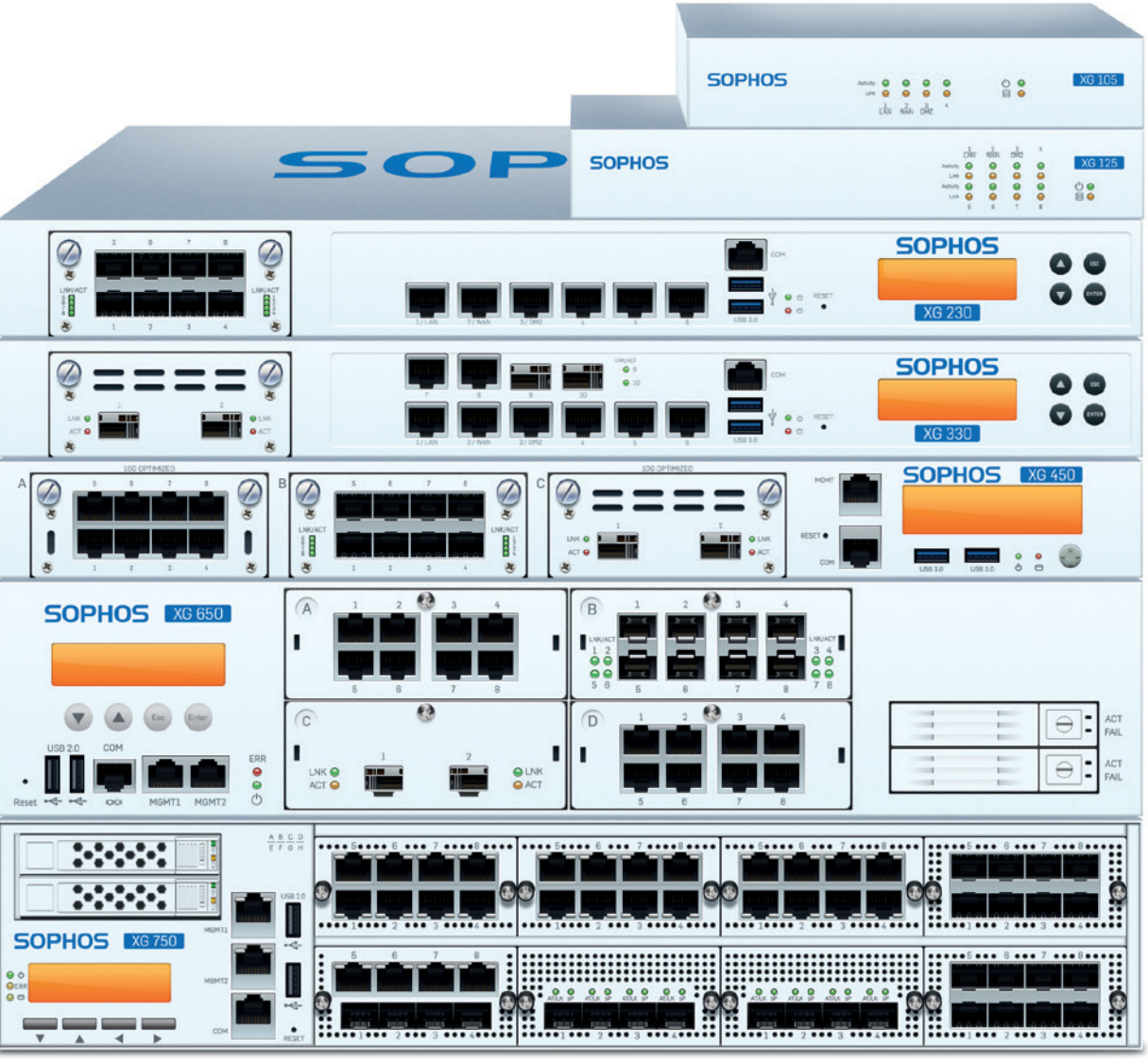
SOPHOS
Security made simple.

サイジングガイド

Sophos XG Firewall – XG シリーズのアプライアンス



最適なアプライアンスを選定するための 3つのステップ

このドキュメントは、最適な Sophos XG シリーズ アプライアンスを選定するためのガイドです。最適なアプライアンスを選択する上で重要なポイントは、さまざまな要因を検討し、ユーザーやネットワーク環境のプロファイル (利用状況の特性) を決定することです。

最適な製品を選定するには、以下のステップを推奨します。

1. UTM 利用ユーザーの総数を把握する
   お客様のウェブ閲覧状況、アプリケーションの利用状況、ネットワーク / サーバーなど、システム環境を理解し、ピーク時の XG シリーズアプライアンスの利用状況を正確に把握します。
2. 機種を選定する

   実効ユーザーの総数から必要な機種を選定します。
3. 特定のスループット要件をチェックする

   インターネットで利用可能な最大アップリンク容量など、ローカル要素がパフォーマンスに影響を与えるかどうかを把握します。Sophos XG Firewall のスループット値と照らし合わせ、推奨機種を選定します。

アプライアンスがお客様の要件を満たしているかどうかを確認するには、お客様の実環境でアプライアンスと Sophos XG Firewall をテストすることが最善の方法であるため、選択したアプライアンスをオンサイトでの無償評価版として提供することもできます。

1.「ユーザー総数」を把握する

以下の表を使用して UTM アプライアンスで処理が必要な、ユーザー総数を算定します。

a. 実効ユーザー数を算定する。ユーザーグループごとに平均的な利用状況にもとづいて相当するカテゴリ (スタンダードユーザー / アドバンスユーザー / パワーユーザー) を判断するか、カテゴリごとに該当するユーザー数を推定します。表 1.2 の基準にもとづいてユーザーをカテゴリ別に分類します。

- 表 1.1 に「ユーザー数」を記入します。対応する係数を掛けて数値を「実効ユーザー数」欄に記入し、各値の合計を「実効ユーザー総数」欄に記入します。
  数式：実効ユーザー総数 = スタンダードユーザー数 X 1 + アドバンスユーザー数 X 1.2 + パワーユーザー数 X 1.5

b. システム負荷値を算定する。表 1.3 の基準にもとづいてシステム負荷を算定します。

- システム負荷の値を「システム負荷値」欄に記入し、「実効ユーザー総数」に「システム負荷値」を掛けた値を「ユーザー総数」欄に記入します。
  数式： ユーザー総数 = 実効ユーザー総数 X システム負荷値

1.1

サポートの種類	ユーザー数	係数	実効ユーザー数
スタンダードユーザー		1	
アドバンスユーザー		1.2	
パワーユーザー		1.5	
ユーザー総数		実効ユーザー総数	
		システム負荷値	
		ユーザー総数	

1.2 ユーザーカテゴリ基準

以下の基準を使用してユーザーの種別を決定します。

	スタンダードユーザー	アドバンスユーザー (*1.2)	パワーユーザー (*1.5)
メールの利用状況 (1日 10時間あたり)			
受信メール数	50通未満	50通～100通	100通以上
データ量	数 MB	数十 MB	数百 MB
Web 利用状況 (1日 10時間あたり)			
データ量	数 MB	数十 MB	数百 MB
使用ピーク発生状況	特になし	数回程度	多い
利用内容	主に Web メール / Google / ニュースサイト	高頻度のネットサーフィン、メディアの転送、業務アプリケーションの利用	きわめて高頻度のネットサーフィン、メディアの転送 (教育機関などにおける)
VPN 利用状況			
VPN リモートアクセス利用状況	ほとんど利用しない – 不定期に接続	週に数回程度 – 定期的に接続	毎日 – ほぼ常時接続

1.3 システム負荷基準

全般的なシステム負荷を増やす可能性のある要件 (性能要件) をすべて割り出します。

	平均レベル	高レベル (*1.2)	最高レベル (*1.5)
Authentication			
Active Directory の利用	×	○	○
FW / IPS / VPN の利用			
IPS (Intrusion Prevention System) で保護するシステム	なし	主に Windows PC、1～2台のサーバー	さまざまなクライアント OS、ブラウザ、マルチメディアアプリケーション、3台以上のサーバー
メール			
スパムの割合	50% 未満	50～90%	90% 以上
レポート			
レポートの保存期間と必要なレポート形式	最大 1か月、Web 形式のレポートのみ (ドメインごと)	最大 3カ月 最大 5件のレポート (ドメインごと)	3カ月以上 (URL ごと)
アプライアンス上のアカウンティングデータの保存期間	×	最大 1カ月	1カ月以上

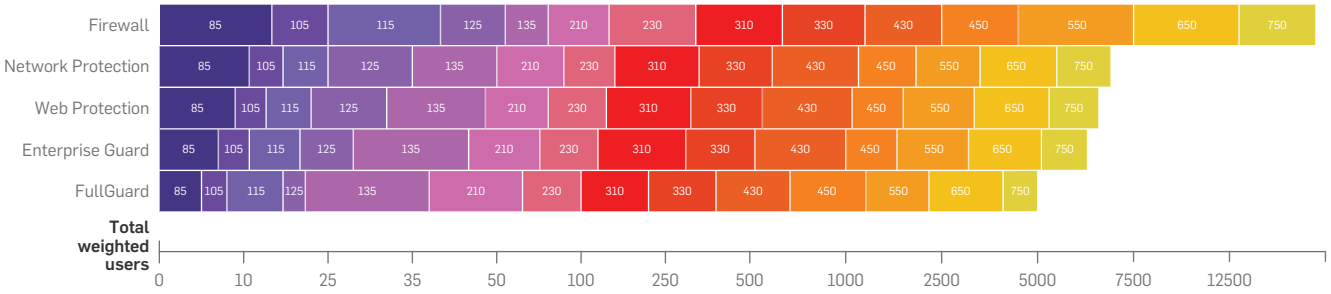
2.「実効ユーザー総数」から機種を選定する

以下の表を使用して「実効ユーザー総数」に該当する XG シリーズ ハードウェア アプライアンスを確認します。

- 「実効ユーザー総数」の目盛りは、各サブスクリプションのみで使用した場合の推奨ユーザー数を表します。
- 利用ユーザーの総数には、必ず VPN、RED、ワイヤレス AP を介して接続するユーザーも含めてください。

サブスクリプションのプロファイル

注:



- Webserver Protection、または Email Protection モジュールを上記のサブスクリプション プロファイルのいずれかに追加する場合は、おおよその目安として実効ユーザー総数を 5%～10% 多く見積もります。※多くの場合、上位機種を選定することをお勧めします。

3.特定のスループット要件をチェックする

お客様の環境によっては、特定のスループット要件があり、初期の見積もりから、より処理能力の高い (または低い) 機器へ見積もりの調整が必要になる場合があります。

特定の要件は、通常次の 2つの要因が原因で発生します。

インターネットで利用可能な最大アップリンク容量

お客様のインターネット接続 (アップリンクおよびダウンリンク) の容量は、選択した機器が転送できる平均的なスループットレートと一致する必要があります (使用しているサブスクリプションによって変わります)。

たとえば、ダウンロードまたはアップロードの上限が 20Mbps のみの場合には、算定したユーザー数が 100 人前後であっても XG 210 の代わりに XG 230 を使用する効果はほとんどありません。この場合には、すべての UTM 機能が有効に設定されていたとしても、インターネット接続に XG 210 で十分に対応できる可能性があります。

ただし、データのフィルタリングはインターネット向けにのみ実行されているとは限らず、社内ネットワークのセグメント間でもフィルタリングが行われる可能性があります。この場合の評価では、ファイアウォールを通過する社内トラフィックも考慮に入れる必要があります。

お客様の使用条件などに基づく特定のパフォーマンス要件

お客様が、接続しているすべての社内および外部のインターフェース全体のスループット要件を (お客様の過去の経験などから) 把握している場合、選択した機器がその数値に対応できるかどうかを確認してください。

たとえば、お客様が DMZ 内にいくつかのサーバーを持ち、すべてのセグメントからの、それらのサーバーへの全トラフィックが IPS によって検査されることが必要である場合があります。または、お客様が多くの異なるネットワークセグメントを持ち、 (ファイアウォール パケットフィルタやアプリケーションコントロール機能を使用して) それらを相互に保護する必要がある場合があります。この場合は、社内のすべてのセグメント間の全トラフィックをスキャンできる機器が必要です。

その他のパフォーマンス上の要件があるかどうかを確認するには、以下の内容を確認します。

- 必要なサイト間 VPN トンネルの数は？
- 1時間あたりのメール転送数 (平均またピーク時) は？
- 生成される Web トラフィック量 (Mbps またはリクエスト/秒、平均またピーク時) は？
- 保護が必要な Web サーバー数および予想されるトラフィック量 (平均またピーク時) は？

以下のセクションに一覧されているパフォーマンスに関する詳細な数値を参考にして、選択したアプライアンスが個別のすべての要件に対応できるかどうかを判断します。

Sophos XG シリーズ ハードウェアのパフォーマンス値

以下の表の値はソフォスのテストラボで計測されたもので、トラフィックタイプ別のパフォーマンス値を一覧にしています。「実環境」の値は、NSS Labs が定義しているように、一般的または現実的なトラフィックとプロトコルの混合による達成可能なスループットの値を示し、「最大」の値は、UDP トラフィックのみで非常に大きなパケットサイズを CPU をフル稼働で使用するなどの理想的な条件で達成可能なスループットを示しています。

お客様が機器を使用する環境は、ユーザーに特殊な条件、使用しているアプリケーション、セキュリティ設定などの要因によって変わってくるため、下記の数字が必ず実現されるわけではありません。このため、これらの数字はサイジングのおおまかな目安としてのみご利用ください。

小規模組織向け - デスクトップ

機種	XG 85/w rev.1	XG 105/w rev.2	XG 115/w rev.2	XG 125/w rev.2	XG 135/w rev.2
パフォーマンスを示す数値					
ファイアウォール最大[1] (Mbps)	2,000	3,000	3,500	5,000	7,000
ファイアウォール IMIX (Mbps)	780	1,040	1,330	1,750	2,750
ファイアウォール実環境[2] (Mbps)	360	430	580	750	1,500
ファイアウォール最大.[1] (パケット/秒)	162,500	243,800	284,500	406,000	569,000
IPS 最大[3] (Mbps)	510	700	900	1,040	1,750
IPS 実環境[2] (Mbps)	75	86	103	180	232
Web プロキシ – AV[5] (Mbps)	330	430	520	590	1,400
Web プロキシ – AV 実環境[2] (Mbps)	75	187	234	307	427
IPS + Web プロキシ – AV 実環境[2] (Mbps)	31	36	42	58	95
NGFW (IPS + App Ctrl + WebFilter) 最大 [3] (Mbps)	235	270	310	360	880
NGFW (IPS + App Ctrl + WebFilter) 実環境 [2] (Mbps)	25	27	30	75	133
VPN AES 最大 [3] (Mbps) 複数トンネル / コア	200	300	350	410	950
VPN AES 最大 [3] (Mbps) 単一トンネル / コア	200	250	290	290	600
VPN AES 実環境 [2] (Mbps) 複数トンネル / コア	50	75	90	105	240
WAF Adv.プロファイル最大[6] (Mbps)	該当なし[6]	12	18	22	44
最大推奨接続数					
新規 TCP 接続/秒	12,000	27,500	27,500	35,000	82,000
同時 TCP 接続数	2,000,000	3,200,000	6,000,000	6,200,000	8,200,000
同時接続 IPsec VPN トンネル数	200	300	500	750	1,000
同時接続 SSL VPN トンネル数	100	200	240	270	270
同時接続アクセスポイント	5	10	20	30	40
同時接続 RED 台数 (UTM/FW)[4]	5/10	10/30	15/60	20/80	25/100
WAF 同時接続仮想サーバー	60[7]	60[7]	60[7]	60[7]	60[7]
WAF 最大接続/秒	700	750	780	950	2,600

1. 1518 バイト パケット サイズ (UDP)
2. データセンター、　企業のネットワーク境界、教育機関、モバイル、金融機関ネットワークプロトコルの混合、50% の CPU 使用率での平均値
3. HTTP トラフィック
4. UTM=XG アプライアンスでの RED トラフィックのフルコンテンツスキャン、FW=パケットフィルタリングのみ
5. 512 キロバイトファイル
6. AV + すべての一般的な脅威対策フィルタと有効 (XG85 では AV なし)
7. ハードコーディングの上限

中規模組織向け- 1U

機種	XG 210 rev.2	XG 230 rev.1	XG 310 rev.1	XG 330 rev.1	XG 430 rev.1	XG 450 rev.1
パフォーマンスを示す数値						
ファイアウォール最大[1] (Mbps)	14,000	18,000	25,000	30,000	37,000	45,000
ファイアウォール IMIX (Mbps)	4,900	6,110	8,530	11,230	12,950	15,650
ファイアウォール実環境[2] (Mbps)	2,060	2,250	3,800	6,100	6,900	7,650
ファイアウォール最大.[1] (パケット/秒)	1,137,800	1,463,000	2,031,860	2,438,200	3,007,200	3,657,400
IPS 最大[3] (Mbps)	2,700	4,200	5,500	8,500	9,000	10,000
IPS 実環境[2] (Mbps)	309	361	539	733	893	1,159
Web プロキシ – AV[5] (Mbps)	2,300	2,800	3,260	6,000	6,500	7,000
Web プロキシ – AV 実環境[2] (Mbps)	538	670	1,140	1,220	1,440	1,690
IPS + Web プロキシ – AV 実環境[2] (Mbps)	102	107	207	242	372	463
NGFW (IPS + App Ctrl + WebFilter) 最大 [3] (Mbps)	1,700	2,420	2,700	4,220	4,800	5,000
NGFW (IPS + App Ctrl + WebFilter) 実環境 [2] (Mbps)	176	226	340	425	538	693
VPN AES 最大 [3] (Mbps) 複数トンネル / コア	1,350	1,500	2,500	3,200	4,800	5,500
VPN AES 最大 [3] (Mbps) 単一トンネル / コア	760	950	990	920	950	990
VPN AES 実環境 [2] (Mbps) 複数トンネル / コア	340	375	625	800	1,200	1,375
WAF Adv.プロファイル最大[6] (Mbps)	205	240	260	510	560	620
最大推奨接続数						
新規 TCP 接続/秒	135,000	140,000	200,000	200,000	200,000	200,000
同時 TCP 接続数	8,200,000	8,200,000	17,500,000	17,500,000	20,000,000	20,000,000
同時接続 IPsec VPN トンネル数	1,300	1,600	1,800	2,500	3,000	3,500
同時接続 SSL VPN トンネル数	300	300	300	300	350	350
同時接続アクセスポイント	75	100	125	150	230	250
同時接続 RED 台数 (UTM/FW)[4]	30/125	40/150	50/200	60/230	70/250	80/300
WAF 同時接続仮想サーバー	60[7]	60[7]	60[7]	60[7]	60[7]	60[7]
WAF 最大接続/秒	3,700	4,200	5,000	9,000	14,000	15,500

1. 1518 バイト パケット サイズ (UDP)
2. データセンター、　企業のネットワーク境界、教育機関、モバイル、金融機関ネットワークプロトコルの混合、50% の CPU 使用率での平均値
3. HTTP トラフィック
4. UTM=XG アプライアンスでの RED トラフィックのフルコンテンツスキャン、FW=パケットフィルタリングのみ
5. 512 キロバイトファイル
6. AV + すべての一般的な脅威対策フィルタと有効 (XG85 では AV なし)
7. ハードコーディングの上限

大規模組織向け - 2U

機種	XG 550 rev.1	XG 650 rev.1	XG 750 rev.1
パフォーマンスを示す数値			
ファイアウォール最大[1] (Mbps)	60,000	80,000	120,000
ファイアウォール IMIX (Mbps)	21,500	26,990	33,500
ファイアウォール実環境[2] (Mbps)	11,700	15,000	19,000
ファイアウォール最大.[1] (パケット/秒)	4,876,500	6,502,000	9,752,900
IPS 最大[3] (Mbps)	13,000	20,000	22,000
IPS 実環境[2] (Mbps)	2,160	3,310	3,970
Web プロキシ – AV[5] (Mbps)	10,000	13,000	17,000
Web プロキシ – AV 実環境[2] (Mbps)	2,480	3,220	3,870
IPS + Web プロキシ – AV 実環境[2] (Mbps)	808	1,109	1,330
NGFW (IPS + App Ctrl + WebFilter) 最大 [3] (Mbps)	8,000	9,000	11,800
NGFW (IPS + App Ctrl + WebFilter) 実環境 [2] (Mbps)	1,190	1,730	2,070
VPN AES 最大 [3] (Mbps) 複数トンネル / コア	8,400	9,000	11,250
VPN AES 最大 [3] (Mbps) 単一トンネル / コア	640	770	620
VPN AES 実環境 [2] (Mbps) 複数トンネル / コア	2,100	2,250	2,800
WAF Adv.プロファイル最大[6] (Mbps)	1,020	1,700	2,460
最大推奨接続数			
新規 TCP 接続/秒	200,000	200,000	300,000
同時 TCP 接続数	20,000,000	20,000,000	30,000,000
同時接続 IPsec VPN トンネル数	4,000	4,500	5,400
同時接続 SSL VPN トンネル数	400	500	500
同時接続アクセスポイント	300	400	500
同時接続 RED 台数 (UTM/FW)[4]	100/400	150/600	200/600*
WAF 同時接続仮想サーバー	60[7]	60[7]	60[7]
WAF 最大接続/秒	18,000	21,000	24,000

*技術的限界

1. 1518 バイト パケット サイズ (UDP)
2. データセンター、　企業のネットワーク境界、教育機関、モバイル、金融機関ネットワークプロトコルの混合、50% の CPU 使用率での平均値
3. HTTP トラフィック
4. UTM=XG アプライアンスでの RED トラフィックのフルコンテンツスキャン、FW=パケットフィルタリングのみ
5. 512 キロバイトファイル
6. AV + すべての一般的な脅威対策フィルタと有効 (XG85 では AV なし)
7. ハードコーディングの上限

Sophos XG Firewall ソフトウェア / 仮想アプライアンス

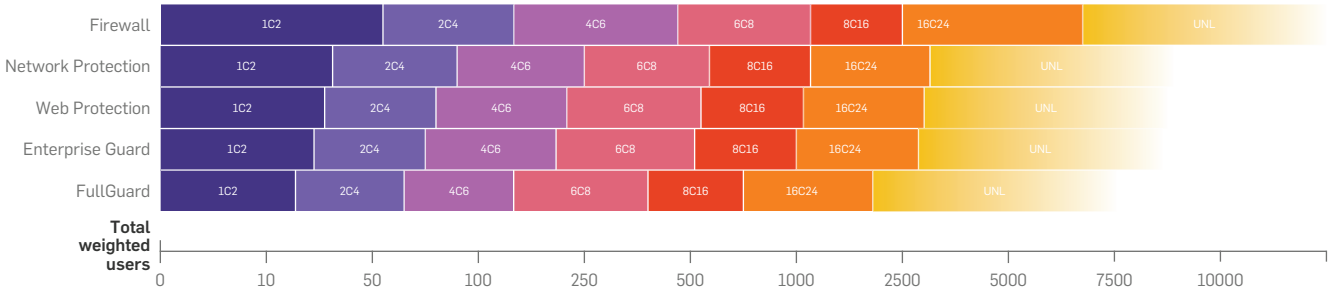
Sophos XG Firewall ソフトウェア / 仮想アプライアンスのライセンスは、(仮想) コア数と (仮想) RAM サイズに基づきます。ライセンスは利用可能なコア / RAM の数に正確に一致する必要はありませんが、ソフトウェア上で使用されるコア / RAM に対してのみライセンスが有効に設定されます。

ソフトウェア / 仮想アプライアンスは、さまざまな速度でさまざまな CPU の種類で使用される可能性があるため、同じ数の コア / RAM サイズで使用する場合でもパフォーマンスが大きく異なる場合もあります。

下記の表には、各ソフトウェアのモデルに推奨される実効ユーザー総数の目安 (第 1章での計算に基づきます) を記載しています。

これ数字は下記の内容を前提にしています。

- CPU 速度 = 2.5 GHz (この値が大きいほど大半のアプリケーションにおけるスループットが大幅に増加します)
- CPU Type = Core I (最大 6C8)、Xeon (8C16 以上)



サブスクリプションのプロファイル

注:

- 仮想環境で Sophos XG Firewall を使用した場合、ハイパーバイザーフレームワークによって最大 10% までのパフォーマンス / ユーザー数の低下が予想されます。

実環境での検証

上記のステップは最適なアプライアンスを選定する基本的な手法です。この方法では、お客様から入手する情報のみがベースになります。アプライアンスの動作やパフォーマンスは多くの要因から影響を受けるため、それらを評価するには実環境と同じシナリオで検証を行う必要があります。このため、実環境での評価は、選定したアプライアンスが実際のパフォーマンス要件を満たしているかどうかを見極める最適な方法です。詳細についてはソフォス株式会社営業部までお問い合わせください。サイジングやプラットフォームの選定を支援します。

無償評価版

30日間の無償試用に登録
http://www.sophos.com/ja-jp/products/

ソフォス株式会社営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

2016-09-21 SG-JA (DD)

SOPHOS