SONICWALL

よくある質問
クライアント DPI-SSL

説明

Secure Socket Layer のディープパケットインスペクション (DPI-SSL) は、SonicWALL のディープパケットインスペクション技術を拡張して、暗号化された HTTPS トラフィックおよび他の SSL ベースのトラフィックにも適用できるようにしたものです。SSL トラフィックが透過的に復号化され、脅威が潜んでいないかスキャンされます。そして、脅威や脆弱性が検出されなければ、トラフィックは再び暗号化されて宛先に送信されます。DPI-SSL は、暗号化された HTTPS および他の SSL ベースのトラフィックを分析するための、追加のセキュリティ、アプリケーション制御、およびデータ漏えい防止機能を提供します。

1. どの SSL アプリケーション / ポートがクライアント DPI-SSL によりプロキシされますか。

次のアプリケーションがクライアント DPI-SSL によりプロキシされます。

HTTPS
FTPS
LDAPS
SMTPS
POPS
IMAP
NNTPS
TelnetS
IRCS

2. カスタム SSL ポートへの接続はクライアント DPI-SSL によりプロキシされますか。

はい。DPI-SSL は、ポート番号にかかわらず SSL トラフィックを調べます。

3. クライアント DPI-SSL が SSL 接続をプロキシするときに使用するのは、どのバージョンの SSL/TLS プロトコルですか。

SSLv3、TLS 1.0 (SSLv31)、および SSLv23 です。

4. クライアント DPI-SSL によりネゴシエートされる、プロキシされた接続の、デフォルトの SSL プロトコルのバージョンは何ですか。

デフォルトでは SSL 3.0 です。これは diag ページで変更できます。 デフォルトプロトコル (SSLv3) を選択した場合、TLS 1.0 以上のみを使用しているサイトへの接続は失敗します。

5. SSLv23 とは何ですか。

SSLv23 は、SonicWall が SSLv3 または TLSv1 のいずれか (サーバーでサポートされている方) とネゴシエーションするときの方式です。

6. デフォルトの DPI-SSL CA 証明書以外の証明書を使用することはできますか。

はい。ただし、デフォルト以外の証明書をクライアント DPI-SSL で再署名用に使用するには、事前に内部 CA 証明書とその秘密鍵を SonicWall にインポートしておく必要があります。 ユーザーはクライアントの DPI-SSL ページの [証明書再署名の認可] のドロップダウンで SonicWall にインポート済みの任意のエンドエンティティ証明書を選択できますが、再署名が確実に行われるようにするには、内部 CA 証明書が必要です。

7. パブリック (またはプライベート) CA から取得した Web サーバー証明書を DPI-SSL クライアントインスペクション用にインポートすることはできますか。

いいえ、できません。上記を参照してください。

8. クライアント DPI-SSL を有効化したところ、ネットワーク内のどのホストでも、HTTPS Web サイトに接続しようとするとブラウザにエラーが表示されます。

SSL 接続の試行時に、クライアント DPI-SSL はトラフィックを傍受し、再署名した証明書をブラウザに提示します。証明書の発行元は、デフォルトの SonicWall DPI-SSL CA 証明書になります。この証明書は、SSL 接続を試みるブラウザまたは他のアプリケーションから信頼されている必要があります。ブラウザに警告が表示されないようにするには、クライアント DPI-SSL 証明書を信頼されている CA としてブラウザの証明書ストアにインポートします。

9. SSL 接続が DPI-SSL によりプロキシされるよう設定してあり、デフォルトのファイアウォール DPI-SSL 証明書を使用しています。にもかかわらず、一部のサイトに接続するときに、自己署名証明書が提示されます。 証明書の発行元フィールドと発行先フィールドには、どちらもサイトの FQDN が表示されています。

SonicWall の背後にあるホストが HTTPS Web サイトにアクセスしようとすると、SonicWall は Web サイトとホストのそれぞれに対して個別に SSL ハンドシェイクを

解決策

1. どの SSL アプリケーション / ポートがクライアント DPI-SSL によりプロキシされますか。
2. カスタム SSL ポートへの接続はクライアント DPI-SSL によりプロキシされますか。
3. クライアント DPI-SSL が SSL 接続をプロキシするときに使用するのは、どのバージョンの SSL/TLS プロトコルですか。
4. クライアント DPI-SSL によりネゴシエートされる、プロキシされた接続の、デフォルトの SSL プロトコルのバージョンは何ですか。
5. SSLv23 とは何ですか。
6. デフォルトの DPI-SSL CA 証明書以外の証明書を使用することはできますか。
7. パブリック CA から取得した Web サーバー証明書を DPI-SSL クライアントインスペクション用にインポートすることはできますか。
8. クライアント DPI-SSL を有効化したところ、ネットワーク内のどのホストでも、HTTPS Web サイトに接続しようとするとブラウザにエラーが表示されます。
9. SSL 接続が DPI-SSL によりプロキシされるよう設定してあり、デフォルトのファイアウォール DPI-SSL 証明書を使用しています。にもかかわらず、一部のサイトに接続するときに、自己署名証明書が提示されます。 証明書の発行元フィールドと発行先フィールドには、どちらもサイトの FQDN が表示されています。
10. DPI-SSL クライアントインスペクションを有効にした状態で一部のサイトをブラウズすると、ページは読み込まれますが、IE の黄色い帯状の領域に「セキュリティ証明書にエラーのあるコンテンツの表示がブロックされました。」というエラーメッセージが表示されます。
11. DPI-SSL では、サイトの証明書が信頼できない場合にそのサイトをブロックできますか。
12. DPI-SSL では特定の SSL トラフィックをプロキシしないようにすることはできますか。
13. クライアント DPI-SSL は、StartTLS コマンドで開始される SSL トラフィックを傍受してプロキシすることはできますか。
14. クライアント DPI-SSL が SSL トラフィックを傍受し、プロキシしているかどうかを確認するにはどうしたらよいですか。
15. DPI-SSL クライアントインスペクションによって復号化されたパケットは、どうすれば表示できますか。
16. SSL トラフィックに対して DPI-SSL が適用されていることをユーザーに警告するには、どうしたらいいですか。
17. UTM アプライアンスがすべてルート (強制トンネル方式) VPN モードで設定されている場合、クライアント DPI-SSL は、GVC クライアントからの SSL トラフィックをプロキシすることができますか。
18. クライアント DPI-SSL CA 証明書を異なる複数の Web ブラウザに配布するにはどうしたらいいですか。
19. クライアント DPI-SSL 証明書をモバイルデバイスに配布するにはどうしたらいいですか。
20. クライアント DPI-SSL 証明書をブラウザ以外のアプリに配布するにはどうしたらいいですか。
21. DPI-SSL クライアントインスペクションがサポートする SSL 接続の最大数はいくつですか。
22. デバイスが最大 SSL 接続数を超えるとどうなりますか。
23. クライアント DPI-SSL の共通名 (CN) による除外リストに追加した Web サイトに最初に接続しようとしたときに切断されてしまうのはなぜですか。

実行します。SonicWall と Web サイト間の SSL ハンドシェイク時に、Web サイトはそのサイトの証明書を提示します。この証明書の CA が SonicWall の証明書ストアに含まれていない場合、SonicWall は自己署名証明書としてその証明書に再署名します。この自己署名証明書はブラウザから信頼されていないため、証明書エラーが発生します。 このエラーを回避するには、欠落しているその Web サイトの CA 証明書 (ルート証明書と中間証明書のいずれかまたは両方) を SonicWall の証明書ストアに手動でインポートします。

10. DPI-SSL クライアントインスペクションを有効にした状態で一部のサイトをブラウズすると、ページは読み込まれますが、IE の黄色い帯状の領域に「セキュリティ証明書にエラーのあるコンテンツの表示がブロックされました。」というエラーメッセージが表示されます。

その Web ページでは、HTTPS を使用して別のサイトに接続するバックグラウンドスクリプトが使用されていますが、そのサイトの CA 証明書が SonicWall の証明書ストアに存在しません。CA 証明書を SonicWall の証明書ストアにインポートしてください。

11. DPI-SSL では、サイトの証明書が信頼できない場合にそのサイトをブロックできますか。

はい。diag ページで、サイトの証明書が信頼できない場合にそのサイトへの接続をブロックするオプションを有効にします。このオプションは、デフォルトでは無効になっています。

12. DPI-SSL では特定の SSL トラフィックをプロキシしないようにすることはできますか。

はい。 管理者は、IP アドレス、ポート、ユーザー、または証明書の共通名 (CN) に基づいて除外を設定できます。

13. クライアント DPI-SSL は、StartTLS コマンドで開始される SSL トラフィックを傍受してプロキシすることはできますか。

はい、できます。最初の 512 バイト (デフォルト) 以内に Client Hello パケットが送信されれば、そのトラフィックがプロキシされます。これは、diag ページの DPI-SSL セクションで変更できます。最大値は 8191 です。

14. クライアント DPI-SSL が SSL トラフィックを傍受し、プロキシしているかどうかを確認するにはどうしたらよいですか。

SonicWall の背後にあるホストで、ブラウザのアドレスバーにある「鍵」のアイコンをクリックして、証明書情報を表示します。クライアント DPI-SSL がその接続をプロキシした場合は、証明書の発行元として、デフォルトまたはカスタムの DPI-SSL CA 証明書が表示されます。

15. DPI-SSL クライアントインスペクションによって復号化されたパケットは、どうすれば表示できますか。

復号化されたパケットは、SonicWall のパケット監視モジュールでキャプチャすることができます。キャプチャを開始する前に、パケット監視の [詳細監視フィルタ] タブにある [中間 SSL 復号化されたトラフィックを監視する] チェックボックスをオンにします。キャプチャされたパケットは、Libpcap、HTML、またはテキストとしてエクスポートできます。

16. SSL トラフィックに対して DPI-SSL が適用されていることをユーザーに警告するには、どうしたらいいですか。

SonicWall が特に推奨する方法はありませんが、そのために CFS 同意ページを導入することはできます。

17. UTM アプライアンスがすべてルート (強制トンネル方式) VPN モードで設定されている場合、クライアント DPI-SSL は、GVC クライアントからの SSL トラフィックをプロキシすることができますか。

GVC クライアントおよび L2TP クライアントの SSL トラフィックは、すべてルート (強制トンネル方式) で設定されていれば、DPI-SSL によりプロキシされます。

18. クライアント DPI-SSL CA 証明書を異なる複数の Web ブラウザに配布するにはどうしたらいいですか。

MS Windows では、Internet Explorer、Chrome、Opera の各ブラウザ間でシステム証明書ストアが共有されます。CA 証明書がローカルコンピュータのストアまたはローカルユーザーのストアに信頼されたルート CA としてインポートされた場合、その CA によって署名されたすべての証明書がこれらのブラウザで信頼されます。Microsoft Certutil コマンドラインユーティリティで次のコマンドを実行することもできます。

certutil -addstore -f -enterprise -user root dpi-ssl.crt > NUL

このプロセスは、グループポリシーなどを使用して自動化することができます。グループポリシーを使用したプロセスの詳細な説明については、次の KB 記事を参照してください。

UTM:「Distributing the Default SonicWall DPI-SSL CA certificate to client computers using Group Policy」

次の個人ブログでは、証明書を exe ファイルとして配布する方法を説明しています。「How to distribute root certificates as exe files」

一方、Mozilla Firefox については、固有の証明書ストアがあるため、CA 証明書をこのストアに手動でインポートする必要があります。または、NSS Certutilutility で次のコマンドを実行することもできます。

certutil -A -n "CN=SonicWall Firewall DPI-SSL" -t C -d C:\Users\\AppData\Roaming\Mozilla\Firefox\Profiles\hbbc3850.default -i dpi-ssl.crt

注 : ここで紹介しているユーティリティはサードパーティのアプリケーションであり、あくまでも CA 証明書の自動導入に使用できる可能性がある多数の方法のうちの 1 つとして紹介しています。SonicWall では、これらのユーティリティの動作状況については責任を負いません。

19. クライアント DPI-SSL 証明書をモバイルデバイスに配布するにはどうしたらいいですか。

サードパーティによる次のブログでは、証明書をモバイルデバイスに配布する方法が説明されています。「Smooth root certificate deployment for mobile devices」

20. クライアント DPI-SSL 証明書をブラウザ以外のアプリに配布するにはどうしたらいいですか。

そのアプリがローカルコンピュータのルート CA 証明書ストアを使用する場合は、ローカルコンピュータのストアに証明書をインポートするだけで済みます。そのアプリ固有の証明書ストアがある場合は、CA 証明書を手動でそのストアにインポートする必要があります。

21. DPI-SSL クライアントインスペクションがサポートする SSL 接続の最大数はいくつですか。

最大数は SonicWall アプライアンスのモデルによって異なります。次の表に、各モデルでサポートされる最大プロキシ接続数を示します。

GEN 6 * ファームウェアバージョン 6.2.5.0 以降が必要		GEN 5 * ファームウェアバージョン 5.9.1.6 以降が必要	
製品	**DPI-SSL 最大同時接続数**	**製品**	**DPI-SSL 最大同時接続数**
SOHO	100	NSA 220/W	100
TZ300	250	NSA 240	100
TZ400	250	NSA 250	100
TZ500	250	NSA 2400	250
TZ600	250	NSA 3500	250
NSA2600	1000	NSA 4500	350
NSA3600	2000	NSA 5000	1000
NSA4600	3000	NSA E5500	2000
NSA5600	4000	NSA E6500	3000
NSA6600	6000	NSA E7500	8000
SM9200	8000	NSA E8500	8000
SM9400	10000		
SM9600	12000		
SM9800	48000 (1 ブレードあたり 24000)		
SM 10200	48000 (1 ブレードあたり 24000)		
SM 10400	96000 (1 ブレードあたり 24000)		
SM 10800	192000 (1 ブレードあたり 24000)		

22. デバイスが最大 SSL 接続数を超えるとどうなりますか。

デフォルトの動作では、DPI-SSL インスペクションなしでトラフィックが許可されます。この動作は、SonicWall の diag ページで、接続数の上限を超えたときにプロキシなしで SSL を許可するオプションを無効にすることによって変更できます。このオプションが無効の場合、SSL 接続数が上限を超えると SSL 接続は切断されます。

23. クライアント DPI-SSL の共通名 (CN) による除外リストに追加した Web サイトに最初に接続しようとしたときに切断されてしまうのはなぜですか。

クライアントが CN による除外対象の Web サイトへの接続を初めて試みるときに、SonicWall はサーバー側の SSL ハンドシェイクを実行して、そのサイトが CN による除外リストに含まれていることを証明書メッセージから検出します。その後、この接続を切断し (SonicWall ではこのハンドシェイクがクライアントとして実行されるため)、証明書の共通名にマップされた IP アドレスをキャッシュします。自動または手動のリフレッシュによる、同じ Web サイトへの 2 回目の接続試行時には、SonicWall は、その接続を DPI-SSL クライアントインスペクションから除外する必要があることを最初のパケット (TCP SYN) 自体から「認識」します。それにより、サーバー側のハンドシェイクを最初からやり直す必要がなくなるため、アプライアンスのリソースを節約できます。

当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、電子メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

FAQ-ClientDPI-EU-IMAG-10764