



SSG 140

次世代スマート・ファイアウォール — ウルトラUTM —

製品概要

ジュニパーネットワークス セキュア・サービス・ゲートウェイ (SSG) 140は、中規模の支社およびビジネスでの導入に適したパフォーマンス、セキュリティ、ルーティング機能を完全に統合した、次世代スマートファイアウォール/VPNです。支社との間のトラフィックは、従来のステートフル・ファイアウォール、IPSec VPNだけでなく、IPS (ディープ・インスペクションFW)、アンチウイルス(アンチスパイウェア)、アンチアドウェア、アンチフィッシングの各機能を含む)、アンチスパム、WebフィルタリングなどのUTM (統合脅威管理) セキュリティ機能により、ワーム、スパイウェア、トロイの木馬、マルウェアから防御されます。

製品説明

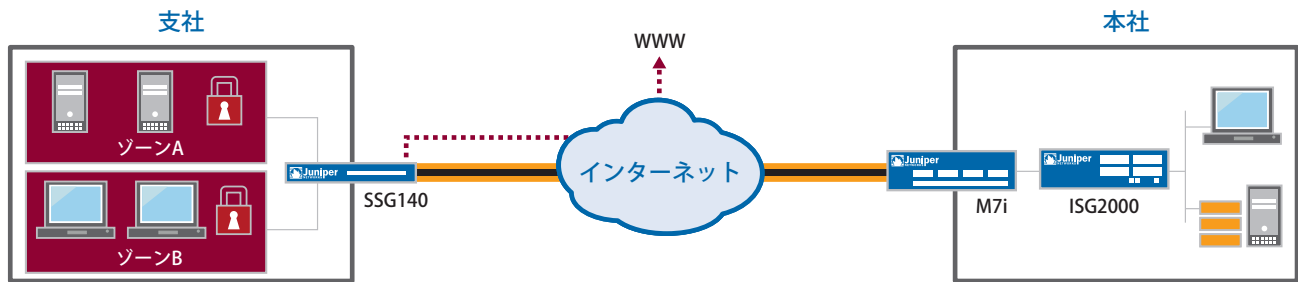
SSG 140は、支店と中小規模拠点向けの高性能なセキュリティ・プラットフォームです。ネットワーク内部と外部からの攻撃を防御し、不正アクセスを拒否するほか、法令遵守を徹底します。SSG 140は、ステートフル・ファイアウォール・トラフィック350 Mbps以上とIPSec VPNスループット100 Mbps以上を提供するモジュール型プラットフォームです。

セキュリティ: 業界最高クラスのパートナー企業から提供されたセキュリティ機能を結集したUTM (統合脅威管理) でワーム、ウイルス、トロイの木馬、スパムなどの新たに登場するマルウェアからネットワークを保護します。内部ネットワークのセキュリティ要件を満たし、法令遵守を徹底するために、セキュリティゾーン、バーチャルルーター、VLANなどの高度なネットワーク保護機能をサポートしています。VLANを使用すると、ネットワークをセキュアドメインに分割し、それぞれにセキュリティポリシーを設定できます。セキュリティゾーンを保護するポリシーには、UTMセキュリティ機能に統合されたアクセス・コントロール・ルールを設定できます。

接続性とルーティング: SSG 140は、インタフェース10ポート (8×10/100と2×10/100/1000) をオンボードに実装しているほか、オプションのWANインタフェースとして、T1、E1、シリアルをサポートするI/O拡張スロット4ポートを備えており、業界最高クラスの拡張性を備えたセキュリティ・プラットフォームです。WANプロトコルとカプセル化に対応した多彩なI/Oインタフェースを備えているため、従来の支店用ルーターとして簡単に導入できるだけでなく、セキュリティ機能とルーティング機能を備えた統合デバイスとして活用すると、設備投資と運用コストを大幅に削減できます。

統合型アクセス・コントロール: SSG 140のプラットフォームは、インフラネット・コントローラを追加するだけでジュニパーネットワークス統合型アクセス・コントロール (UAC) ソリューションのインフラネット・エンフォーサとして動作します。中央ポリシー管理エンジンであるインフラネット・コントローラは、SSG 140と通信して、ファイアウォール・ベースのアクセス/コントロールを補強するか、より詳細な基準に基づいてアクセスを許可または拒否するソリューションに変更します。インフラネット・コントローラは、エンドポイントの状態とユーザーアカウント (個人属性も含むアカウント情報) を評価し、臨機応変なポリシー管理をネットワーク全域にリアルタイムで実行します。

業界最高レベルのサポート: ジュニパーネットワークスのプロフェッショナルサービスは、研究所における簡単な試験から大規模なネットワークの実装まで、幅広い技術サポートを提供しています。お客様のITチームと協力して、プロジェクトの目標を設定し、導入プロセスの定義、ネットワーク設計の作成と検証、配置管理を行います。



SSG 140を支店に導入して、セキュアなインターネット接続と本社とのVPN接続を構築します。
支店のリソースは、セキュリティポリシーを各セキュリティゾーンに設定して保護します。

機能と利点

機能	機能解説	利点
高性能	専用のハードウェア、高い処理能力、セキュリティ専用オペレーティングシステムを組み合わせたセキュリティ専用プラットフォーム	現在の環境と将来的な拡張を視野に入れて、ネットワーク内外からの脅威を確実に防御
業界最高クラスの UTM セキュリティ機能	UTMセキュリティ機能（アンチウイルス、アンチスパム、Webフィルタリング、IPS）であらゆるウイルスとマルウェアによるネットワーク攻撃を未然に阻止	あらゆる攻撃からネットワークを保護
統合型アンチウイルス	Kaspersky Lab社のアンチ・ウイルス・エンジンをジュニパーネットワークスが提供（別途年間ライセンスが必要です）	ウイルス、スパイウェア、アドウェアなどのマルウェアの侵入を防御
統合型アンチスパム	Symantec社のアンチスパム製品をジュニパーネットワークスが提供（別途年間ライセンスが必要です）	既知のスパムやフィッシャーが送信した電子メールをブロック
統合型 Web フィルタリング	SurfControl社のWebフィルタリング・ソリューションをジュニパーネットワークスが提供（別途年間ライセンスが必要です）	悪意あるWebサイトへのアクセスを制御またはブロック
統合型侵入検知防御（ディープ・インスペクション）	IPSエンジン（別途年間ライセンスが必要です）	アプリケーションレベルに対するフラッド攻撃を防御
固定インタフェース	10/100インタフェース（固定）×8、10/100/1000インタフェース×2、USBポート×1、コンソールポート×1、AUXポート×1	高速なLAN接続、拡張性に優れた接続性、柔軟な管理機能を提供
ネットワークのセグメント化	ブリッジグループ、セキュリティゾーン、仮想LAN、バーチャルルーターにセキュリティポリシーを設定し、ゲスト、無線ネットワーク、拠点サーバー、データベースを分離	内部ネットワーク、外部ネットワーク、ネットワーク上のサブグループに配置した非武装セグメント（DMZ）にセキュリティ機能を迅速に導入して不正アクセスを防御
堅牢なルーティングエンジン	OSPF、BGP、RIP v1/2、フレームリレー、マルチリンク・フレーム・リレー、PPP、マルチリンクPPP、HDLCに対応した定評あるルーティングエンジン	セキュリティ機能とルーティング機能を統合し、運用費用と設備投資を削減
高密度のインタフェース	10/100インタフェース×8、10/100/1000インタフェース×2、管理用ポート（コンソールポート×1、AUXインタフェース×1）	競合製品に比べて、圧倒的なインタフェース密度を誇る
モジュール型インタフェース	SSG 140の拡張ポート4個は、オプションとして、T1、E1、シリアル物理インタフェースモジュール（PIM）、10/100/1000、SFPユニバーサルPIM（uPIM）接続に対応	抜群のセキュリティ機能を備えたLAN/WAN接続を提供し、運用費用を削減し、既存の投資を保護
柔軟なネットワーク管理	コマンドライン・インタフェース（CLI）、WebUIまたはジュニパーネットワークスNetwork and Security Manager（NSM）を使用したセキュリティポリシーの確実な導入、監視、管理	任意のロケーションから管理機能にアクセス可能。現場に向かず、ネットワークを管理できるため、レスポンス時間を短縮して、運用費用を削減できる
ジュニパーネットワークス統合型アクセス・コントロールのインフラネット・エンフォーサ	中央ポリシー管理エンジン（インフラネット・コントローラ）と対話し、ユーザーアイデンティティ、デバイスのセキュリティ状態、ネットワークロケーションに基づき、セッション固有のアクセス・コントロール・ポリシーを実行	お客様の既存のネットワークインフラと業界最高レベルの技術を活用して、セキュリティをコスト効果的に強化
業界最高レベルのプロフェッショナルサービス	ジュニパーネットワークスのプロフェッショナルサービスは、研究所における簡単な試験から大規模なネットワーク実装までの広範なサポートサービスを提供。お客様のITチームと協力して、プロジェクトの目標を設定し、導入プロセスの定義、ネットワーク設計の作成と検証、配置管理を実施	ネットワークインフラのセキュリティ、柔軟性、拡張性、信頼性を保証
Auto-Connect-VPN	ハブアンドスポーク型トポロジのスポークサイト間でVPNトンネルを自動的に設定/停止	VoIPビデオ会議など、遅延が許されないアプリケーションのメッシュ型トポロジに拡張性の優れたVPNソリューションを提供

製品オプション

オプション	オプション解説
DRAM	512 MBのDRAMを搭載
UTM/ コンテンツセキュリティ (ハイメモリオプション)	SSG 140は業界最高クラスのUTMとコンテンツセキュリティ機能を提供します。アンチウイルス (アンチスパイウェア、アンチフィッシング)、IPS (ディープ・インスペクション)、Webフィルタリング、アンチスパムを利用できます。
I/O オプション	SSG 140インタフェースの拡張スロット4個は、T1、E1、シリアル物理インタフェース (PIM)、10/100/1000、SFPユニバーサルPIM (uPIM) 接続をオプションとしてサポートしています。



仕様

最大パフォーマンス・設定数⁽¹⁾

ScreenOSバージョンチェック	ScreenOS 6.2
ファイアウォール・パフォーマンス (ラージパケット)	350Mbps以上
ファイアウォール・パフォーマンス (IMIX) ⁽²⁾	300Mbps
ファイアウォールパケット/秒 (64バイト)	100,000PPS
AES (米次世代暗号標準、256ビット) + SHA-1 VPNのスループット	100Mbps
3DES暗号化 + SHA-1 VPNのスループット	100Mbps
最大同時セッション数	48,000
新規セッション数/秒	8,000
最大セキュリティポリシー数	1000
最大サポートユーザー数	無制限

ネットワーク接続

固定I/O	8×10/100、 2×10/100/1000
物理インタフェースモジュール (PIM) スロット数	4
モジュール型WAN/LAN インタフェースのオプション (PIM/uPIM)	2×T1、2×E1、 2×シリアル、 1×ISDN BRI S/T SFP、 10/100/1000

ファイアウォール

ネットワーク攻撃検知	<input type="radio"/>
DoS/DDoS攻撃防御	<input type="radio"/>
TCPパケット再構成による フラグメントパケット攻撃防御	<input type="radio"/>
総当たり攻撃緩和	<input type="radio"/>
Syn Cookie防御	<input type="radio"/>
ゾーンベースIPスプーフィング	<input type="radio"/>
異常パケット攻撃防御	<input type="radio"/>

UTM⁽³⁾

IPS (ディープ・インスペクション・ ファイアウォール)	<input type="radio"/>
プロトコル異常検知	<input type="radio"/>
ステートフル・プロトコル・シグネチャ	<input type="radio"/>
アンチウイルス	<input type="radio"/>
シグネチャデータベース	200,000以上
対応プロトコル	POP3、HTTP、SMTP、 IMAP、FTP、IM
アンチスパイウェア	<input type="radio"/>
アンチアドウェア	<input type="radio"/>
アンチキーロガー	<input type="radio"/>
インスタントメッセージAV	<input type="radio"/>
アンチスパム	<input type="radio"/>
統合型URLフィルタリング	<input type="radio"/>
外部URLフィルタリング ⁽⁴⁾	<input type="radio"/>

VoIPセキュリティ

H.323対応アプリケーション・レベル・ ゲートウェイ (ALG)	<input type="radio"/>
SIP ALG	<input type="radio"/>
MGCP ALG	<input type="radio"/>
SCCP ALG	<input type="radio"/>
Network Address Translation (NAT) for VoIP protocols	<input type="radio"/>

IPSec VPN

同時VPNトンネル数	500
トンネル用インタフェース数	50
DES暗号化 (56ビット)、 3DES暗号化 (168ビット)、AES (256ビット)	<input type="radio"/>
MD-5/SHA-1認証	<input type="radio"/>
手動鍵、IKE、PKI (X.509)	<input type="radio"/>
PFS (DHグループ)	1、2、5
リプレイ攻撃防御	<input type="radio"/>
リモートアクセスVPN	<input type="radio"/>
IPSec内のL2TP利用	<input type="radio"/>
IPSec NATトラバース	<input type="radio"/>
Auto-Connect-VPN	<input type="radio"/>
VPNゲートウェイ冗長化	<input type="radio"/>

ユーザー認証とアクセス・コントロール

組み込み（内部）データベース（ユーザー制限用）	250
外部認証	RADIUS、RSA SecureID、LDAP
RADIUSアカウントリング	○、起動/停止
XAUTH VPN認証	○
ウェブベースの認証	○
802.1X認証	○
統合型アクセス・コントロール（UAC）対応 インフラネット・エンフォーサ	○

PKIサポート

PKI証明書要求（PKCS 7、PKCS 10）	○
自動証明書登録（SCEP）	○
OCSF（Online Certificate Status Protocol）	○
対応認証局	VeriSign、Entrust、Microsoft、RSA Keon、iPlanet（Netscape）、Baltimore、DoD PKI
自己署名証明書	○

バーチャリゼーション

セキュリティゾーン最大数	40
バーチャルルーター最大数	6
ブリッジグループ	○
最大VLAN数	100

ルーティング

BGPインスタンス	6
BGPピア	24
最大BGPルート数	2,048
OSPFインスタンス	3
最大OSPFルート数	2,048
RIP v1/v2インスタンス	64
最大RIP v2ルート数	2,048
最大ルーティングエントリ数	2,048
ソースベース・ルーティング	○
ポリシーベース・ルーティング	○
ECMP（等価コストマルチパス）	○
マルチキャスト	○
リバース・フォワーディング・パス（RFP）	○
IGMP（Internet Group Management Protocol）（v1、v2）	○
IGMP Proxy	○
プロトコル独立マルチキャスト（PIM） シングルモード	○
PIMソース・スペシフィック・ マルチキャスト	○
マルチキャスト内IPSecトンネル	○

カプセル化

PPP（Point-to-Point Protocol）	○
MLPPP（Multilink Point-to-Point Protocol）	○
MLPPP最大物理インタフェース数	4
フレームリレー	○
MLFR（Multilink Frame Relay） （FRF 15、FRF 16）	○
MLFR最大物理インタフェース数	4
HDLC	○

IPv6

IPv4/IPv6ファイアウォールとVPNのデュアル スタック	○
IPv4とIPv6の変換とカプセル化	○
Syn-CookieとSyn-ProxylによるDoS攻撃検出	○
SIP、RTSP、Sun-RPC、MS-RPC ALG	○
RIPng	○
BGP	○
透過モード	○
NSRP	○
DHCPv6リレー	○

動作モード

レイヤ2（透過）モード ⁽⁵⁾	○
レイヤ3（ルート/NAT）モード	○

アドレス変換

NAT（ネットワークアドレス変換）	○
PAT（ポートアドレス変換）	○
ポリシーベースNAT/PAT （レイヤー2、レイヤー3モード）	○
MIP（IPマッピング、レイヤー3モード）	1,500
VIP（バーチャルIP、レイヤー3モード）	16
MIP/VIPグルーピング（レイヤー3モード）	○

IPアドレス割り当て

静的割り当て	○
DHCP、PPPoEクライアント	○
内部DHCPサーバー	○
DHCPリレー	○

トラフィック管理とサービス品質（QoS）

帯域保証	○（ポリシー単位）
最大帯域	○（ポリシー単位）
受信トラフィックのポリシング	○
優先帯域利用	○
DiffServeマーキング	○（ポリシー単位）

高可用性（HA）

アクティブ/アクティブ構成 - L3モード	○
アクティブ/パッシブ構成 - 透過モードと L3モード	○
コンフィグレーション同期	○
ファイアウォール/VPNセッション同期	○
ルーティング変更の為のセッション・ フェイルオーバー	○
VRRP	○
デバイス障害検知	○
リンク障害検知	○
新規HAメンバーの認証	○
HAトラフィックの暗号化	○

システム管理	
ウェブ・ユーザーインターフェース (HTTP/HTTPS)	○
コマンドライン・インターフェース (コンソール)	○
コマンドライン・インターフェース (telnet)	○
コマンドライン・インターフェース (SSH)	○ (v1.5およびv2.0互換)
Network and Security Manager (NSM)	○
インターフェース上でVPNトンネル経由の管理	○
ラピッド・ディプロイメント機能	×

運用管理	
ローカル管理者データベースサイズ	20
管理者用外部データベースサポート	RADIUS、RSA SecurID、LDAP
管理者専用ネットワーク	6
Root Admin、Admin、Read Onlyの各ユーザーレベル	○
ソフトウェアアップグレード	TFTP、WebUI、NSM、SCP、USB
コンフィグレーション・ロールバック	○

ログ収集・モニタリング	
Syslog (複数サーバー)	○、最大4サーバー
Eメール (2アドレス)	○
NetIQ WebTrends	○
SNMP (v2)	○
SNMP用のフルカスタムMIB	○
Traceroute	○
VPNトンネルモニター	○

外部フラッシュメモリ	
ログストレージ増設	USB 1.1
イベントログ/アラーム	○
システムコンフィグ・スクリプト	○
ScreenOSソフトウェア	○

寸法・電源仕様	
寸法 (幅×高さ×奥行き)	44.5×4.5×38.1 cm
重量	4.63 Kg
ラックマウント対応	○ (1RU)
電源 (AC) ⁽⁶⁾	AC入力電圧、動作範囲：100~240VAC AC入力ライン周波数 50/60Hz ACシステム電流定格 2A
最大熱出力	580 BTU/時 (170W)
騒音値	48.8dB

準拠規格	
安全規格	UL、CUL、CSA、CB
EMC規格	FCC class B、CE class B
NEBS	×
MTBF (Bellcoreモデル)	16年

セキュリティ準拠規格	
共通基準 (CC) : EAL4	取得予定
FIPS 140-2 : レベル2	取得予定
ICSA (Firewall/VPN)	○

動作環境	
動作時温度範囲	0°C~50°C
非動作時温度範囲	-20°C~70°C
湿度範囲	10~90% (結露しないこと)

- 実際の数値はScreenOSのバージョンや導入環境によって異なることがあります。
- IMIXは、インターネット・ミックス (Internet Mix) の略語です。実運用環境では、単一サイズのバケットだけという状況は少なく、さまざまなサイズのバケットが混在しているのが一般的です。このような条件では、単一サイズのバケットだけの環境よりもはるかに高い処理能力が求められます。そのような実運用環境を想定したトラフィックをIMIXトラフィックと呼びます。弊社が採用するIMIXトラフィックは、64バイト長が58.33%、570バイト長が33.33%、1518バイト長が8.33%の割合のUDPトラフィックです。
- 各UTM機能 (IPS (ディープ・インスペクションFW)、アンチウィルス、アンチスパム、統合型URLフィルタリング) は、別途ジュニアネットワークスとの年間ライセンス契約が必要です。このライセンス契約により、各シグネチャのアップデートやサポートが提供されます。
- Webフィルタリングのリダイレクト機能は、ファイアウォールから受信したトラフィックをセカンダリサーバーに送ります。リダイレクト機能は無料ですが、Websense社またはSurfControl社のWebフィルタリング・ライセンスを別途購入する必要があります。
- NAT、PAT、ポリシーベースのNAT、バーチャルIP、マップIP、バーチャルシステム、バーチャルルーター、VLAN、OSPF、BGP、RIPv2、アクティブ/アクティブHA、IPアドレス割当ては、レイヤ2透過モードでは使用できません。
- 日本向けに出荷される製品付属のAC電源コードは100V専用です。

IPS (ディープ・インスペクションFW) シグネチャパック

シグネチャパックでは、配置方法と攻撃タイプに応じて、防御方法を調整できます。SSG 140で利用できるシグネチャパックは、次のとおりです。

シグネチャパック	導入対象	防御タイプ	標的タイプ
ベース	支社、中小企業	クライアント/サーバー、ワーム保護	各種シグネチャ、プロトコル異常
クライアント	リモートオフィス、支店	境界防御、ホストのコンプライアンス (デスクトップなど)	サーバーからクライアントへの攻撃
サーバー	中小企業	境界防御、サーバーインフラのコンプライアンス	クライアントからサーバーへの攻撃
ワーム攻撃緩和	大企業の支店、リモートオフィス	ワーム攻撃に対する総合的な防御	ワーム、トロイの木馬、バックドア攻撃

高性能をもたらすサービスとサポート

ジュニパーネットワークスは、高性能な製品によってサービスとサポートをもたらすリーダーであり、高性能ネットワークの促進や拡張、最適化の実現に向けたサービスを提供しています。これらのサービスでは、オンラインで迅速に収益創出能力を提供することにより、生産性の向上や、新しいビジネスモデルおよびベンチャー事業の迅速な展開、市場参入の拡大などを実現するとともに、より高いレベルの顧客満足度を達成します。また、ネットワークを最適化することで、必要な性能レベルや信頼性、可用性を維持し、オペレーショナル・エクセレンス（卓越した運用）を保証しています。

詳細については、<http://www.juniper.net/jp/products-services/>をご参照ください。

ジュニパーネットワークスについて

ジュニパーネットワークスは、ハイ・パフォーマンス・ネットワークキングのリーダーです。サービスおよびアプリケーションの一元化されたネットワークにおける展開を加速するのに不可欠な、即応性と信頼性の高い環境を構築するハイ・パフォーマンスなネットワーク・インフラストラクチャを提供するジュニパーネットワークスは、お客様のビジネス・パフォーマンスの向上に貢献します。ジュニパーネットワークスに関する詳細な情報は、以下のURLでご覧になれます。

<http://www.juniper.net/jp/>

日本

ジュニパーネットワークス株式会社
東京本社
〒163-1035
東京都新宿区西新宿3-7-1
新宿パークタワーN棟35階
電話 03-5321-2600
FAX 03-5321-2700

西日本事務所
〒541-0041
大阪府大阪市中央区北浜1-1-27
グランクリュ大阪北浜

<http://www.juniper.net/jp/>

米国本社

Juniper Networks, Inc.
1194 North Mathilda Ave
Sunnyvale, CA 94089
USA

電話 888-JUNIPER
(888-586-4737)
または408-745-2000
FAX 408-745-2100

URL <http://www.juniper.net>

アジアパシフィック

Juniper Networks (Hong Kong) Ltd.
26/F
Cityplaza One
1111 King's Road,
Taikoo Shing, Hong Kong

電話 852-2332-3636
FAX 852-2574-7803

ヨーロッパ、中東、アフリカ

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin
Ireland

電話 35-31-8903-600
FAX 35-31-8903-601

Copyright © 2009, Juniper Networks, Inc. All rights reserved.

Juniper Networks、JUNOS、NetScreen、ScreenOS、Juniper Networksロゴ、およびJUNOSelは、米国およびその他の国におけるJuniper Networks Inc.の登録商標または商標です。また、その他記載されているすべての商標、サービスマーク、登録商標、登録サービスマークは、各所有者に所有権があります。ジュニパーネットワークスは、本資料の記載内容に誤りがあった場合、一切責任を負いません。ジュニパーネットワークスは、本発行物を予告なく変更、修正、転載、または改訂する権利を有します。

1000181-002 JP May 2009