

NetScreen-5000シリーズ



NETSCREEN®
Scalable Security Solutions



特長：

- **多機能セキュリティシステム**
ステートフル・インスペクション・ファイアウォール、堅牢なDoS攻撃防御、ハイパフォーマンスIPSec VPN、トラフィック管理機能を搭載した統合ネットワークセキュリティソリューション
- **モジュラ+シャーシ型システム**
大規模エンタプライズや通信事業者用に設計された柔軟性と拡張性を備えたハイパフォーマンスな特定用途向けの統合セキュリティシステム
- **抜群のパフォーマンス**
最大12Gbpsのファイアウォールパフォーマンスと最大6GbpsのVPNパフォーマンス
- **バーチャルシステム**
システムを個別のエンティティ（トラフィック、ポリシー、管理）に論理分割することで、1システムで多数部門、多数顧客のセキュリティ保護を実現

製品概要

セキュリティシステム「NetScreen-5000シリーズ」には、2スロット仕様の「NetScreen-5200」と4スロット仕様の「NetScreen-5400」が用意され、大規模エンタプライズや通信事業者またはデータセンタ等に比類のないハイパフォーマンスを提供します。ネットスクリーン独自の第三世代セキュリティ技術であるASICと分散型システム構造を核として、拡張性と柔軟性に優れたネットワークセキュリティシステムを実現しました。

NetScreen-5000システムアーキテクチャには連携して動作する複数のプロセッシングモジュールを使用し、多彩なセキュリティ・ゲートウェイ・インタフェースやパフォーマンス構成を提供します。モジュールにはポート構成が異なる各種セキュリティ・プロセッシング・モジュールやシステム全体を制御するマネージメントモジュールがあり、これらを種々に組み合わせて特定の顧客環境にシステムをカスタマイズできます。NetScreen-5000シリーズは、データ交換用スイッチファブリックと制御情報用の独立した複数のバスチャネルを採用し、厳しいトラフィック条件下においてもスケーラブルなパフォーマンスを発揮できます。

NetScreen-5000シリーズは高い信頼性を維持するために耐障害性に優れたコンポーネントを使用しています。電源部はホットスワップおよびロードシェアリングをサポートし、システムの「N+1」バックアップを可能にします。ファン部は交換式エアフィルタを備えたホットスワップ対応モジュールに予備ファンを備える仕様となります。

ネットスクリーン独自のGigaScreen-II ASIC

ネットスクリーン社の第三世代セキュリティASIC「GigaScreen-II」は独立しに動作し、フルパケット・プロセッシング・エンジンとして、パケットの解析、分類、暗号/復号化、NAT、セッションマッチング等の先端機能をギガビットのスループットで提供します。

NetScreen-5000システムはこの高速な処理能力をスイッチファブリックと直接内部で結合させることで真にスケーラブルなセキュリティソリューションを提供します。

セキュアポートモジュール

セキュアポートモジュールは1または複数のGigaScreen-II ASICを中心に設計され、各種ネットワークインタフェースを介してステートフルインスペクションやIPSec VPN等の中核機能を提供します。また複数のポートを束ね隣接ネットワークエレメントに多重伝送するマルチギガビット接続や、10/100Mbpsやギガビットイーサネット（GigE）インタフェースにセキュリティプロセッシング能力を組み合わせる多彩なコンフィグレーションも可能です。セキュリティポートモジュールを追加することで拡張性問題を解決でき、同時にマネージメントモジュールの処理負担を軽減してシステム全体の制御に集中することを可能にします。

マネージメントモジュール

NetScreen-5000シリーズの各製品にはシステムの全体制御や構成機能を提供するマネージメントモジュールが搭載されています。管理機能の制御は2基のシリアルポートまたは専用の10/100 Ethernetポートを介して実行されます。またセキュアポートモジュール上の1または複数のインタフェースを介して包括的管理オプションにインバンド接続でアクセスすることも可能です。マネージメントモジュールはさらにログ、コンフィグ、ファームウェアイメージ等の情報を保管する外部コンパクトフラッシュや、網冗長構成時におけるHA（High Availability）トラフィックのためのGigabit Ethernet専用ポートを2基装備しています。

NetScreen ScreenOS

NetScreenのScreenOSはシステム全体にわたるファームウェアであり、その中核部には極めてセキュアかつハイパフォーマンスなシステムを実現する基本設計時から作り込まれたカスタムデザインのリアルタイムOSが使用されています。最大パフォーマンスを発揮できるようNetScreenセキュリティ・アプリケーション&システムを最適化し、下記を含む数多くの機能を搭載し、かつ操作性に優れたプラットフォームを提供します。

- ICSA認定のステートフル・インスペクション・ファイアウォール
- ICSA認定のIPSec VPNゲートウェイ
- セキュリティ、ネットワーク、管理機能のバーチャル化
- ネットワークの高信頼性を実現するHA (High Availability)
- 豊富なマネージメントインタフェース (Internal/External)

ファイアウォール機能

多彩な機能を凝縮したネットスクリーン社のファイアウォールは外部や内部からの攻撃に対するセキュリティ技術にステートフルインスペクションをベースとする技術を採用しています。各物理および仮想インタフェースはDoS攻撃防御機能をサポートします。他にも以下の特徴により今日のネットワークに要求される柔軟性とセキュリティを備えています。

- セキュリティを重視したハードウェア、OS、ファイアウォールで構成された統合型ソリューション。携帯性に劣るソフトウェア型ソリューションに比べ高水準のセキュリティおよびパフォーマンスを実現。
- SYN攻撃、ICMP Flood、ポートスキャン等を含む拡張版DoS攻撃防御機能。ハードウェアと結合した高速のセッションエンジニアリング機能により高負荷のネットワーク環境でも優れた防御機能を発揮します。
- ネットワークアドレス変換 (NAT) やポートアドレス変換 (PAT) —これらはルーティングに使用できない内部IPアドレスを第2層のIPセキュリティブリッジのデバイス機能である透過モードのように保護します。

VPN

NetScreen-5000はステートフル・インスペクション・ファイアウォールに加え豊富な機能を搭載したVPNソリューションを提供します。VPNトンネルを任意のインタフェースで開始または終了して、先進のVPNネットワークを展開できます。ScreenOSが持つ統合性は復号化したVPNトラフィックを完全に検査し、さらに転送が必要であれば再度暗号化することも可能です。たとえば、大規模ネットワークでの単一システムによる複数ネットワークセグメントの防御、無線LANセグメント等の暗号化による機密性の確保、セグメント間の継続的なトラフィック検査の実現を実現します。

NetScreen-5000の動作はネットワーク間のゲートウェイとして、あるいはセキュアモバイルまたはワイヤレスWANコネクションの一方と顧客ネットワークのVPNコネクションの他方とを終端するキャリアの通信環境に相当します。本ソリューションはまた以下の機能を提供します。

- リモートアクセス用の総合型VPN
- 拡張版サイト間VPN通信

バーチャリゼーション(仮想システム、VLAN、セキュリティゾーン)

NetScreenセキュリティシステムはシステムを複数のエンティティに論理分割し、トラフィック、ポリシー、管理をそれぞれ独立化するバーチャリゼーション機能を提供します。トラフィックの分割は交換網との統合を容易にするために802.1Q VLANを介してインタフェースレベルで実施します。セキュリティゾーンでは仮想インタフェースと物理インタフェースの両方またはいずれかが内部の論理ネットワークにグループ化されます。次にポリシーがこれらのゾーン間に適用され、複数インタフェースからの類似トラフィックを1つのポリシーで容易に制御します。

最後に、トラフィックと管理機能を完全に分離し独立したデバイスセットとして機能させるために、バーチャルシステムを生成して複数の論理デバイスを構成します。このバーチャリゼーション機能は複数の顧客または企業内部のセキュリティを1つのシステムに収容し、個々のデバイスのセキュリティを損なわずにネットワークの展開や管理の簡素化を実現します。

High Availability

NetScreen-5000システムの各ペアは、構成情報、Activeファイアウォールのセッションテーブル、VPN接続を同期させ、耐障害性に優れた冗長型のネットワーク設計を可能にします。2つの同一デバイスのうち一方をActive、他方をPassiveとして構成すれば、デバイス障害が発生してもネットワーク運用にほとんど影響を及ぼしません。また2002年の第三四半期にはネットスクリーン High AvailabilityソリューションNSRPv2がサポートされる予定です。同エンハンス版ソリューションはサブセカンドフェイルオーバーのActive/Active機能を提供する他、フルメッシュ構成をサポートします。High Availabilityソリューションは、現在市販されている他社セキュリティ製品と異なり、NetScreenセキュリティシステムに標準装備されます。

トラフィック管理

NetScreen-5000システムはセキュアポートモジュールにおける各インタフェースのハードウェア処理レートを制限することで、ネットワークのトラフィックが集中しても正確な伝送帯域の共有を可能にします。IPヘッダのDiffServスタンプはポリシーコントロール下で設定され、各エンジン部により各転送パケットのQoSを提供します。

総合管理

NetScreenセキュリティシステムはネットワーク運用者のセキュアデバイス管理を支援する強力な管理機能を提供します。VPN機能のビルトインにより管理情報は暗号化され真にセキュアなリモート管理を実現します。以下に主な管理機能を示します。

- Web UI (HTTP/HTTPS) をビルトインしたBrowserベースの管理
- セキュアコマンドシェル (SSH v.1互換)、TELNET、コンソールポートを使用するコマンドラインインタフェース (CLI)
- 電子メールアラート、SNMPアラーム
- SyslogまたはWebTrends™との統合による外部ログの収集、監視、分析
- 最大20の管理者に3段階のアクセス権 (Root Admin、Admin、Read-Only) を設定。ネットスクリーン独自のポリシーベース管理「NetScreen-Global PRO」との連携によりキメ細かな制御が可能
- 1バーチャルシステム毎にユニークな管理ログインを設定することで、システム管理者はWebUIまたはCLIへの管理アクセスをパーティション可能
- NetScreen-Global PROまたはNetScreen-Global PRO Expressを使用したポリシーベースの集中管理と監視

NetScreen-5000シリーズの性能⁽¹⁾

特徴	NetScreen-5200	NetScreen-5400
同時セッション数	1,000,000 (2)	1,000,000 (2)
新規セッション数/秒	25,000	25,000
ファイアウォールパフォーマンス	4 Gbps (最大)	12 Gbps (最大)
Triple-DES (168ビット) パフォーマンス	2 Gbps (最大)	6 Gbps (最大)
ポリシー数	40,000 (4)	40,000 (4)
ルール数	200,000 (4)	200,000 (4)
スロット数	2	4
トラフィックインタフェース数	2 mini-GBIC(SX又はLX), 24 x 10/100 または8 mini-GBIC (SX又はLX) モジュール	最大6 mini-GBIC (SX又はLX), 72 10/100 または24 mini-GBIC (SX又はLX) モジュール

NetScreen-5000シリーズの特徴⁽¹⁾

バーチャル化

最大バーチャルシステム数	500
最大セキュリティゾーン数	1,000
最大バーチャルルーター数	500
VLANサポート数	4,000

動作モード

透過モード (全インタフェース)	Yes
ルートモード (全インタフェース)	Yes
NAT (ネットワークアドレス変換)	インタフェース単位
ポリシー型NAT	Yes
PAT (ポートアドレス変換)	Yes
Virtual IP数	8 (6)
Mapped IP数	4000 (4)
IPルーティング静的ルート数	4000 (4)
1ポート当たりのユーザー数	無制限

ファイアウォールアタック検出 (インタフェース単位)

SYN Flood検出	Yes(3)
ICMP Flood検出	Yes(3)
UDP Flood検出	Yes(3)
Ping of Death検出	Yes
IP Spoofing検出	Yes
Port Scan検出	Yes(3)
Land Attack検出	Yes
Tear Drop Attack検出	Yes
Filter IP Source Route オプション	Yes
IP Address Sweep Attack検出	Yes
WinNuke Attack検出	Yes
Java/ActiveX/Zip/EXE	Yes
Default Packet Deny	Yes
User-Defined Malicious URL	Yes, 64
Per-source session limiting	Yes
SYN Fragment	Yes
SYN and FIN Bit Set	Yes
No flags in TCP	Yes
FIN with no ACK	Yes
ICMP Fragment	Yes
Large ICMP	Yes
IP Source Route	Yes
IP Record Route	Yes
IP Securityオプション	Yes
IPタイムスタンプ	Yes
IPストリーム	Yes
IP Badオプション	Yes
Unknownプロトコル	Yes

トラフィック管理

保証帯域幅	No
最大帯域幅	Yes
優先帯域幅利用	No
DiffServスタンプ	Yes

ファイアウォール& VPNユーザー認証

ビルトイン (内部) データベース/ユーザー制限	25,000
RADIUS (外部) データベース	Yes
RSA SecureID (外部) データベース	Yes
LDAP (外部) データベース	Yes

外部フラッシュカード

小型フラッシュ	128MB、512MBサンディスク
イベントログおよびアラーム	Yes
システムconfigスクリプト	Yes
ScreenOSソフトウェア	Yes

VPN

専用VPNトンネル数	25,000 (4)
Manual Key、IKE、PKI (X.509)	Yes
3DES (168-bit)、AES (128-bit)、DES (56-bit)	Yes
Perfect Forward Secrecy (DHグループ)	1,2,5
リプレイ攻撃防御	Yes
リモートVPN接続	Yes
IPSec区間内L2TP	Yes
サイト間VPN接続	Yes
スター型 (Hub&Spoke) VPN網構成	Yes
IPSec NAT Traversal	Yes

IPSec認証

SHA-1	Yes
MD5	Yes
PKI証明書申請 (PKCS 7 & PKCS 10)	Yes
Automated Certificate Enrollment (SCEP)	Yes
Online Certificate Status Protocol (OCSP)	Yes
サポート認証局	
VeriSign CA	Yes
Entrust CA	Yes
Microsoft CA	Yes
RSA Keon CA	Yes
iPlanet (Netscape) CA	Yes
Baltimore CA	Yes
DOD PKI CA	Yes

ハイアベラビリティ(HA)

Active/ActiveフルメッシュHA+NSRP v2	Future ScreenOS
Active/Passive完全同期型HA	Yes
Firewall&VPNセッション保護	Yes
デバイス障害検出	Yes
リンク障害検出	Yes
フェールオーバー時の網通知	Yes
New HA Members認証	Yes
HAトラフィックの暗号化	Yes

システム管理

WebUI (HTTP & HTTPS)	Yes
CLI (Console)	Yes
CLI (Telnet)	Yes
Secure Command Shell (SSH v1互換)	Yes
NetScreen-Global PRO	Yes(5)
NetScreen-Global PRO Express	Yes(5)
VPNトンネル経由のインタフェース管理	Yes
SNMPフルカスタム版MIB	Yes

管理

管理者数	20
リモート管理者DB	RADIUS
管理用ネットワーク	6
アクセス権 (Root Admin, Admin, Read Only User)	Yes
ソフトウェアアップグレード & コンフィグ変更	TFTP/WebUI/Global
スケジューラ	256

ロギング/監視

Syslog	External
E-mail通知 (2アドレス)	Yes
NetIQ WebTrends	External
SNMP	Yes
Traceroute	Yes
VPNトンネル監視	Yes
Websense URL Filtering	External

(1) NetScreen ScreenOS 3.1.0r1のパフォーマンス、キャパシティ、特徴 (他のNetScreen Screen OSリリース製品と仕様異なります)

(2) 1セキアポートカード当たりの最小キャパシティ (ハードウェア構成により異なります)

(3) 物理インタフェースのみ仮想インタフェースは物理インタフェースのプロパティを継承します。

(4) バーチャルシステム間で共有

(5) NetScreen-Global PRO/PRO Express version 3.2でサポートされるNetScreen-5000

(6) 仮想システムでは利用できません

仕様とオーダー情報

仕様：

サポート標準

ARP, TCP/IP, UDP, ICMP, HTTP, RADIUS, IPSec (IPESP, IPAH), MD5, SHA1, DES, 3DES, AES, IKE, TFTP (client), SNMP, X.509v3, VLAN 802.1q

NetScreen-5200の諸元および動作環境

848 x 483 x 572 (HxWxD mm)、19インチ筐体、2U、前面・背面・中央いずれも実装可
電源は背面パネル、他はすべて前面パネル操作
動作時温度：0 ~ 40℃
保管時温度：-20 ~ 70℃
相対湿度：10 ~ 90% 結露なし
最大熱放散：510 BTU/時 (150W)
平均熱放散：300 BTU/時 (87W)
重量：37ポンド

交流電源仕様

入力電圧：90 ~ 264 VAC
入力周波数：47 ~ 63 HZ、(自動調整)
最大入力電流：3A (100VAC)
最大出力：150W DC

直流電源仕様

入力電圧：-36 ~ -60VDC
公称入力電圧：-48VDC
最大入力電流：6A (-36VDC)
最大出力：150W DC

NetScreen-5400の諸元および動作環境

219 x 483 x 349 (HxWxD mm)、19インチ筐体、5U、前面実装のみ
すべて前面パネル操作
重量：45ポンド

NetScreen-5200 認証規格

GR-63-Core：NEBS, Environmental Testing Physical Protection
GR-1089-Core：EMC and Electrical Safety for Network Telecommunications Equipment

安全規格：

UL, CUL, CSA, CB, Austel

EMI規格：

FCC class A, BSMI, CE class A, C-Tick, VCCI class A

オーダー情報：

製品

NetScreen-5200 Bundles

製品	パーツ番号
NetScreen-5200, 8 GigE SPM, 0 VSYS, AC	NS-5200-P01A-S00
NetScreen-5200, 8 GigE SPM, 0 VSYS, DC	NS-5200-P01D-S00
NetScreen-5200, 8 GigE SPM, 100 VSYS, AC	NS-5200-P01A-S01
NetScreen-5200, 8 GigE SPM, 100 VSYS, DC	NS-5200-P01D-S01
NetScreen-5200, 8 GigE SPM, 500 VSYS, AC	NS-5200-P01A-S02
NetScreen-5200, 8 GigE SPM, 500 VSYS, DC	NS-5200-P01D-S02

Virtual Systems

NetScreen-5000 VSYS Upgrade 0 to 5	NS-5000-VSYS-5
NetScreen-5000 VSYS Upgrade 5 to 25	NS-5000-VSYS-25
NetScreen-5000 VSYS Upgrade 25 to 50	NS-5000-VSYS-50
NetScreen-5000 VSYS Upgrade 50 to 100	NS-5000-VSYS-100
NetScreen-5000 VSYS Upgrade 100 to 250	NS-5000-VSYS-250
NetScreen-5000 VSYS Upgrade 250 to 500	NS-5000-VSYS-500
NetScreen-5000 VSYS Upgrade 0 to 500	NS-5000-VSYS

NetScreen-5000 Components

Management Module	NS-5000-MGT
8 GigE Secure Port Module (SPM)	NS-5000-8G
mini-GBIC transceiver - SX	NS-SYS-GBIC-MSX
mini-GBIC transceiver - LX	NS-SYS-GBIC-MLX

NetScreen-5200 Components

NetScreen-5200 Chassis	NS-5200-CHA
NetScreen-5200 AC Power Supply	NS-5200-PWR-AC
NetScreen-5200 DC Power Supply	NS-5200-PWR-DC
NetScreen-5200 Fan Assembly	NS-5200-FAN

*NetScreen-5400と24-port 10/100セキュア・ポート・モジュールの両方またはいずれかを含むシステムパッケージおよびコンポーネントはこれらの製品の出荷開始と同時に利用可能になります。

NetScreenの製品保証とサービス

NetScreen社は標準保証サービスとして、ハードウェア製品に関しては1年間、ソフトウェア製品に関しては90日間の保証を提供します。年間保守契約も用意されており、最新ソフトウェアを継続してご利用いただきエンドユーザーシステムのハイアベイラビリティを実現しています。NetScreen社はまたコンサルティング、設置、設定等を含む「プロフェッショナルサービス」をはじめ、トレーニングや認定書発行等のプログラムも用意しています。



ネットスクリーン・テクノロジーズ・ジャパン株式会社

〒107-0052 東京都港区赤坂2-21-15 赤坂OSビル4F

電話：03-6229-2685

FAX：03-6229-2686

www.netscreen.com

Copyright © 1998-2002 NetScreen Technologies, Inc.

NetScreen、NetScreen Technologies、NetScreenロゴはNetScreen Technologies社の登録商標です。NetScreen-5XP、NetScreen-25、NetScreen-50、NetScreen-100、NetScreen-204、NetScreen-208、NetScreen-500、NetScreen-1000、NetScreen-5200、NetScreen-5400、NetScreen-Global PRO、NetScreen-Global PRO Express、NetScreen-Remote、GigaScreen ASIC、GigaScreen ASIC II、NetScreen ScreenOSはNetScreen Technologies社の商標です。その他、本カタログ中の会社名、商品名は各社の商標および登録商標です。

Part Number：2002.4.3.1.5000.jp