

Cisco Secure PIX Firewall シリーズ

以前 PIX Firewall として知られていた Cisco Secure PIX[®] Firewall シリーズは、インストールが簡単で卓越した性能を備えた統合型ハードウェア/ソフトウェア機器によって、強力なセキュリティを提供します。このシリーズ製品を使用することにより、外部の侵入から内部ネットワークを厳重に保護できる、完全なファイアウォール・セキュリティ保護機能が得られます。

企業ネットワークの非パラレル・セキュリティ

Cisco Secure PIX Firewall シリーズは、インストールが簡単で卓越した性能を備えた統合型ハードウェア/ソフトウェア機器によって、強力なセキュリティ機能を提供します。このシリーズ製品を使用することにより、外部の侵入から内部ネットワークを厳重に保護できる、完全なファイアウォール・セキュリティ保護機能が得られます。アプリケーション・レベルで各データパケットを拡張処理する一般的な CPU 中心のフルタイム・プロキシ・サーバと異なり、Cisco Secure PIX Firewall は、非 UNIX の安全なリアルタイムの組み込みシステムを使用します。PIX Firewall は、最大で 256,000 の同時接続、1 秒間に 6,500 以上の接続、およそ 170Mbps のスループットを可能とする優れた性能を備えています。この性能レベルは、他の機器型ファイアウォールや汎用オペレーティングシステムに基づいたファイアウォールの性能に比べてはるかに優れています。

図 1 : Cisco Secure PIX Firewall シリーズ



VPN 相互運用性と IPSec とのスケラビリティ

従来のファイアウォールは、接続されたネットワーク・セグメント間のすべての接続に対してステートフルな制御を維持することにより、境界セキュリティを提供するものでした。最近では、アクセス制御だけでなく、VPN (仮想プライベートネットワーク) サービスに対してもファイアウォールを要求する顧客が増えています。IP 層で実現する VPN に対して、インターネット技術特別調査委員会 (IETF) IP Security ワーキング・グループは、IPSec と呼ばれる複数標準の草案を作成しました。

この新たに登場した IETF IPSec 標準は、インターネットやあらゆる IP ネットワークを通じた安全なプライベート通信を実現することを目的としています。IPSec によって、機密性、完全性、認証の確実性が確保されます。IOS/IPSec に組み込まれて動作し、Cisco ルータ、またはバージョン 5.0 以降の PIX (1999 年発売) に対応する IPSec 暗号化機能を使用することにより、複数のエンドポイント間での安全な VPN をサポートできます。たとえば、リモートまたはモバイル型 Windows PC と、VPN クライアント・ソフトウェア、Cisco IOS ルータ、その他の PIX Firewall、または IPSec 準拠の暗号化デバイスとの間の VPN が挙げられます。

IPSec に基づいた VPN により、リモートユーザーは、離れたクライアント・コンピュータからでも企業ネットワークに低価格で安全にアクセスできます。インターネットを利用してアクセスすれば、従来の専用線または専用ネットワークに必要なとされた電気通信コストを大幅に削減できます。さらに、企業はリモートユーザーのアクセスを処理するために、大規模なモデムバンクとアクセスサーバを維持する必要がなくなり、高額な資本投資と管理上の問題に頭を悩ますこともありません。ISP に市内電話をかけるだけで、ユーザーはインターネットから企業のプライベート・イントラネットに安全にアクセスできます。

IPSec は、セキュリティおよび認証プロトコルと、最も重要なインターネット・キー交換 (IKE) の保護を対象としています。IKE により、2 つのエンドポイントは事前共有キーまたは公開キー・インフラストラクチャ (PKI) のデジタル認証を使用して、安全な接続を確立できます。このデジタル認証は、公開キーを登録する社内またはアウトソース・サービスの認証権限者により管理されます。IKE により、VPN は、署名入りのデジタル ID カードと同等の機能を使用して各エンドポイントを認証するので、数千ものエンドポイントに拡張できます。

データの暗号化を確実にするため、シスコは、ルータと PIX に IPSec を採用して、データ暗号規格 (DES) および Triple DES アルゴリズムの両方をサポートしています。現時点で、これら IPSec 準拠製品の 56 ビット DES バージョンを、米国から世界各国の顧客に輸出できます。168 ビットの Triple DES 製品も輸出可能ですが、56 ビット DES よりも厳しい輸出規制があります。最新の輸出規制情報については、シスコの販売担当者にお問い合わせください。

プラットフォームの拡張性

組み込みシステムの利点を損なうことなく必要なプラットフォームの拡張性を提供するために、Cisco Secure PIX Firewall シリーズは、PIX Firewall 515 および 520 の 2 つのハードウェア・プラットフォームを備えています。これらは、広範囲にわたるネットワークインタフェースカード (NIC) をサポートしています。標準 NIC には、単一ポートまたは 4 ポートの 10/100 イーサネットカード、4/16 トークンリングカード、およびデュアル・アタッチのマルチモード FDDI カードが用意されています。FDDI カードおよび 4 ポート・イーサネットカードは、バージョン 4.4 以降の PIX でサポートされています。

DC 電源によるファイアウォール・ソリューションを必要とするサイトの場合、PIX Firewall 520 は現在、48VDC 電源での使用が可能です。PIX Firewall 520-DC は、Bellcore GR-63 および GR-1089 標準テストにおいて NEBS レベル 3 と認定されました。

グラフィカルなインストールと管理

Cisco Secure PIX Firewallシリーズは、インストールと管理の手順を簡易化するために、Setup Wizardと、グラフィカルなFirewall Managerを備えています。Setup Wizardは、Windows 95およびWindows NTで動作するグラフィカルなプログラムで、PIX Firewallの初期インストールを素早く実行できるようにします。Firewall Managerを使用することにより、ネットワーク管理者は、直観的なグラフィカル・ユーザー・インタフェース (GUI) を使用して、簡単にPIX Firewallをコンフィギュレーションおよび管理できます。目的のPIX Firewallを示すアイコンをクリックするだけで、セキュリティ・ポリシーを検索、編集し、一元的に管理できます。

各種の管理レポートにより、ネットワーク管理者は、不正なユーザー、トラフィック量、予想されるコスト会計に関する統計分析を行えます。さらにネットワーク管理者は、URLログを監査して、どのWebサイトが最もアクセス頻度が高いかをモニタリングできます。また、しきい値を設定することにより、ファイアウォールがハッカーに攻撃された時点でリアルタイム警告を電子メールまたはポケットベルで自動受信できます。

いくつかのサード・パーティ製品をCisco Secure PIX Firewallと併用することにより、さらに管理レポートの拡張機能を利用できます。オープン・システム・ソリューションのPrivate Iにより、1つまたは複数のPIX Firewallの継続的なモニタリングに基づいた標準的な日常のオペレーション・レポートを網羅できます。ユーザーはカスタマイズ・レポートを作成することもできます。TelemateソフトウェアのTelemate.Netは、ファイアウォール・ログを分析して、インターネット使用量レコードとユーザーおよび部門のディレクトリとを照合します。Telemate.Netレポートを使用して、ユーザーの使用コストを追跡し、そのコストをユーザーに請求できます。

こうしたレポート機能のほかに、PIX FirewallはアクティブにURLをフィルタリングして、ユーザーがアクセス可能なWebサイトを制御します。URLのフィルタリング機能は、現在、Cisco PIX Firewallのバージョンで、NetPartners WebSENSEサーバ・ソフトウェアと統合することにより実行できます。WebSENSEサーバは、Windows NT上か、ネットワーク内またはPIX Firewall外の保護された周辺ネットワークに設置されたUNIXサーバ上のいずれかで動作します。URLフィルタリングは個別のプラットフォームで処理されるので、ファイアウォールとURLフィルタリングを同じプラットフォームで稼働する競合製品のファイアウォールのように、PIX Firewallの性能を大きく阻害することがありません。

最高のパフォーマンスと接続数

Cisco Secure PIX Firewallシリーズの高いパフォーマンスを特徴付ける機能のひとつは、アダプティブ・セキュリティ・アルゴリズム (ASA) に基づいた保護方式です。この保護方式は、受信および送信パケットをテーブル内のエントリと比較することにより、内部ホスト・ネットワークへのアクセスを効果的に保護します。通過検証を行うための適切な接続が存在する場合にのみ、アクセスが許可されます。もう一つの特徴的な機能は、認証精度を向上させるカッター・プロキシです。カッター・プロキシは最初のアプリケーション層でユーザーをチェックします。

ユーザーが認証され、ポリシーがチェックされた後は、PIX Firewallによりセッション・フローが低位レイヤに移動し、格段に速い処理性能が得られます。

Cisco Secure PIX Firewall 515-R (制限付きモデル) は最大で64,000の同時セッション、PIX 515-UR (無制限モデル) は最大で128,000の同時セッション、PIX 520は最大で256,000の同時セッションをサポートします。これらの各PIXモデルは、エンドユーザー性能に影響を及ぼすことなく数千のユーザーを収容することができます。KeyLabs社が実施した各種Firebenchテストによれば、フル装備のPIX Firewallは、競合製品よりも高速で動作し、より多くの同時接続が可能です。この一連テストにより、PIX Firewallは1秒間で6,579接続を安全に受容し、169MbpsのFTPおよびHTTPトラフィック送信を行えることが実証されました。これは高速のキャンパスLANまたは複数のT3 WAN環境を十分にサポートできる性能です。これらは、汎用オペレーティングシステムに基づく競合製品のファイアウォールが実現する速度の2~3倍の速度です。

最強のセキュリティと管理の容易性

こうした高レベルの性能以外に、PIX Firewallのリアルタイムの組み込みシステムにより、Cisco Secure PIX Firewallシリーズの安全性も向上します。UNIXサーバは広く使用できるソースコードを備え、オープン開発プラットフォームとしては最適ですが、こうした汎用オペレーティングシステムでは性能と安全性の最適化を実現することはできません。Cisco Secure PIX Firewallシリーズは、安全性が高く、高性能な保護機能を実現することを目的とする専用製品として設計されています。

さらに信頼性を高めるために、Cisco Secure PIX Firewallシリーズはフェールオーバー/ホットスタンバイ・アップグレード・オプションを備えています。このオプションにより、シングル・ポイントの障害を排除できます。2つのPIX Firewallが並行して動作することにより、どちらかが故障した場合に、セカンダリPIX Firewallが自動的にセキュリティ・オペレーションを維持します。

管理者は、Firewall Manager ツールを使用して、複数のPIX Firewallを1か所で簡単にコンフィギュレーションおよび管理できます。一般的なセキュリティ・ポリシーを、わずか6つのコマンドで実装できます。日常的な管理作業はほとんど必要ないので、継続的なメンテナンス作業が大幅に軽減されます。

図2: Firewall Manager ユーザーインタフェース



グラフィカルな Firewall Manager を使用して、複数の PIX Firewall を 1 か所で簡単に設定および管理することができます。また、アカウントングレポートを生成できるので、部門別にコスト請求することなども可能になります。

Java 対応のブラウザから Windows NT システムで稼働する Firewall Manager にアクセスするだけで、コンフィギュレーションを簡易化できます。システムが認証され接続されたら、ネットワーク上のすべての PIX Firewall を示すグラフィックが、ウィンドウ内の 1 か所に表示されます。ウィンドウの別の個所には、使用可能なコンフィギュレーション・コマンド・リストが表示されます。Cisco Secure PIX Firewall をクリックした後、該当するコンフィギュレーション機能を選択して、ファイアウォールのコンフィギュレーションを開始します。あるいは、Cisco IOS ユーザーインターフェースに慣れているユーザーは、同じようなソフトウェア・ベースのコマンド行インターフェースを選択することもできます。

また、Firewall Manager は、Cisco Secure PIX Firewall シリーズのアクティビティを分析し、報告する際にも使用できます。Cisco Secure または他の TACACS+ や RADIUS サーバに関して、接続日時、合計接続時間と送受信された合計バイト数、ユーザーごとのスループット (バイトまたはパケット)、アプリケーション・ミックス (ポート数)、その他の重要データに関する情報を記載するアカウントングレポートを生成できます。様々な目的、たとえば各部門別へのコスト請求に、会計レポートを使用できます。

制御を最大化するコンテンツ別機能

安全なデータベース・アクセスを可能にするため、Cisco Secure PIX Firewall シリーズでは、Oracle SQL*Net ベースのクライアント / サーバ・アプリケーションが、ネットワークアドレス変換 (NAT) の使用に関わらずファイアウォールを通して通信することができます。この業界初の機能により、モバイルユーザーはファイアウォールに守られた企業情報サーバにアクセスすることができます。さらにこの機能は、電子商取引においてベンダと顧客をリンクしたり、安全なエクストラネットの展開を容易にします。

悪意のある Java アプレットの脅威をできるだけ排除するために、Cisco Secure PIX Firewall シリーズは Java アプレット・フィルタを装備しています。このフィルタにより、HTTP を介して送信された (アーカイブやその他の方法で圧縮されていない) Java アプレットを阻止できるので、悪意による攻撃を制限できます。サードパーティ製品とともに使用することにより、Java および ActiveX のもっとも高度なフィルタリング機能が得られます。

内部メールホストへのダイレクトなメール転送を安全に実現する機能である Mail Guard により、受信トラフィックの内容がより強力に制御されるため、高コストのメールリレーホストが必要なくなります。Mail Guard により、TCP ポート 25 からのみ、内部メールホストへの接続が可能です。また、すべての SMTP (簡易メール転送プロトコル) のアクティビティのログが記録され、RFC 821 の Section 4.5.1. に記載の最小の SMTP サーバコマンドのみが許可されます。サードパーティ製品とともに使用すると、より高度なメールのフィルタリング機能が得られます。

マネージド・ファイアウォール・サービスに理想的

サービスプロバイダーは、Cisco Secure PIX Firewall シリーズを使用することにより、柔軟性のあるスケーラブルな管理ファイアウォール・サービスを構築できます。コンフィギュレーションおよび管理の簡単さと統合化されたハードウェアおよびソフトウェア設計によって、PIX Firewall を顧客宅内機器 (CPE) としてセントラル・オフィス (CO) に展開する場合も、ローカル POP に展開する場合も、作業が簡略化されます。シャーシ内のあらゆるインターフェースを通じてロギングおよびコンフィギュレーションのアップデートが可能となるため、サービスプロバイダーはすべての PIX Firewall をリモート管理することができます。DC 電源によるファイアウォール・ソリューションを必要とする CO または POP の場合、Cisco Secure PIX Firewall 520 は現在、-48VDC 電源でのみご使用いただけます。Cisco Secure PIX Firewall 520-DC は、Bellcore GR-63 および GR-1089 標準テストにおいて NEBS レベル 3 と認定されました。

IP アドレス不足時の対処

Cisco Secure PIX Firewall シリーズには、IP アドレスの不足を懸念することなく、IP ネットワークを拡大および再設定する機能が用意されています。NAT により、既存の IP アドレス、または IANA リザーブ・プール (RFC 1918) に確保された予備のアドレスのいずれも使用できます。Cisco Secure PIX Firewall シリーズでは、さらに、必要に応じてアドレス・ミックスを変換するかどうかを選択できます。NAT は、マルチメディア・アプリケーションのサポートなどの他のすべての PIX Firewall の機能とともに使用できるようになっています。競合製品のファイアウォールでは、マルチメディアと NAT は相互に排他的な機能です。

Cisco Secure PIX Firewall シリーズは、「ポートレベルの多重化」を行うポートアドレス変換 (PAT) をサポートし、より多くの IP アドレスを利用できます。PAT により、ユーザーの内部ローカルアドレスが単一の外部ローカルアドレスに自動変換され、それぞれの変換を区別するために異なるポート番号が使用されます。64,000 以上の内部ホストを単一の外部 IP アドレスでまかなうことができます。

未登録のアドレスが、登録済みアドレスの IP アドレス・スペースと重複する場合、Net Aliasing ソフトウェアによってそれぞれのアドレスがどのネットワークに属しているかが追跡され、データが適切なネットワークに送信されるようにします。

機能と利点の要約

Cisco Secure PIX Firewall シリーズ ソフトウェア V.4.4 の機能と利点

機能	利点
アダプティブ・セキュリティ・アルゴリズム	すべてのTCP/IPセッションにステートフルなセキュリティを提供し、機密性のあるプライベート・リソースを保護します。
カットスルー・プロキシ	業界最高の認証性能を提供します。既存の認証データベースを再使用することにより、所有コストを低減します。
安全なリアルタイムの組み込みシステム	UNIXやNTワークステーションなどの標準に基づいたオープン・オペレーティングシステムよりも強力なセキュリティを提供します。
複数のネットワークインタフェースカード	Webやその他の公共アクセスが可能なサーバ、異なるパートナーにリンクする複数のエクストラネット、保護ロギング、URLフィルタリング・サーバなどに対して、強力なセキュリティを提供します。
サービス拒絶攻撃を防止	ファイアウォールとサーバ、およびその中のクライアントをハッカーの攻撃から保護します。サービス拒絶攻撃に対して、すべてのトランザクションとサービスの安全性を確保します。
最大で256,000の同時接続をサポート	プロキシ・サーバをはるかに凌ぐ性能により、展開するファイアウォール数が減少します。
IETF IPsecサポート	VPNの相互運用性、スケーラビリティ、管理コストの低減を実現します。
広範囲にわたるアプリケーションのサポート (TCP/IPプロトコルに示された全リスト、および、仕様に示されたアプリケーション・サポートを参照してください。)	ファイアウォールによるネットワーク・ユーザーへの影響を少なくします。
PIX Firewall ManagerおよびSetup Wizard	ネットワークのダウンタイム縮小による時間とコストの削減、インストール・コストの削減。
管理レポート:URLアカウンティング	アカウンティングデータなどのPIX Firewallのアクティビティを簡単に参照できるため、時間を節約します。
URLフィルタリング	ユーザーがアクセスするWebサイトを制御し、アカウンティングのために監査・トラッキングを行う機能を備えています。PIX Firewall性能に与える影響を最小限に留めます。
Java Applet Filter	ファイアウォールが、潜在的な危険性を有するJavaアプリケーションを、クライアント別またはIPアドレス別に停止できるようにします。
Mail Guard	周辺ネットワーク内で外部メール・リレーを使用する必要がなくなるので、外部メール・リレーへのサービス拒絶攻撃を排除できます。
マルチメディア・アプリケーションのサポート	これらのプロトコルをサポートする際に必要な管理の時間とコストを削減します。特別なクライアント・コンフィギュレーションは必要ありません。
フェールオーバー/ホット・スタンバイ	ネットワークの信頼性を最大化する高いアベイラビリティをもたらします。
ネットワークアドレス変換	IPの再マッピングにかかる高額のコストを削減します。ネットワークアドレスのスペースを拡大します。
非変換 認証/監査	既存のIPアドレスを使用して、強力なセキュリティを備えたクライアントIDを作成できます。サード・パーティによりセキュリティ強度を検証します (ICSA認証、SRIIによるセキュリティ監査、NSA Common Criteria認証 検証中)

Cisco Secure PIX Firewall シリーズ仕様

ハードウェア・プラットフォームおよび仕様

	PIX Firewall 515-R	PIX Firewall 515-UR	PIX Firewall 520	PIX Firewall 520-DC
ハードウェア・ケース	19インチ、ラックマウント可能 (ラックマウント・ハードウェアに付属)	19インチ、ラックマウント可能 (ラックマウント・ハードウェアに付属)	19インチ、ラックマウント可能 (ラックマウント・ハードウェアに付属)	19インチ、ラックマウント可能 (ラックマウント・ハードウェアに付属)
ランダム・アクセス・メモリ	32MB	64MB	128MB	128MB
フラッシュメモリ	16MB	16MB	16MB	16MB
コンソール・ポート	RJ-45	RJ-45	DB-9 EIA/TIA-232	DB-9 EIA/TIA-232
ブート/アップデート・デバイス	TFTPのみ	TFTPのみ	3.5インチ フロッピーディスクドライブ	3.5インチ フロッピーディスクドライブ
フェールオーバー・ポート ¹	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232
物理寸法				
高さ	1.72"	1.72"	5.21インチ	5.21インチ
幅	16.82インチ	16.82インチ	16.82インチ	16.82インチ
奥行き	11.8インチ	11.8インチ	17.5インチ	17.5インチ
重量	4.99kg	4.99kg	9.53kg	9.53kg
電力要件				
自動スイッチング	100 ~ 220VAC	100 ~ 240VAC	100 ~ 240VAC	- 48VDC
周波数	50 ~ 60Hz	50 ~ 60Hz	50 ~ 60Hz	---
電流	1.5 ~ 0.75Amp	1.5 ~ 0.75Amp	4 ~ 2Amp	4Amp
動作環境				
動作温度	- 5 ~ +45 (-25 ~ 113 F)	- 5 ~ +45 (-25 ~ 113 F)	- 5 ~ +45 (-25 ~ 113 F)	- 5 ~ +45 (-25 ~ 113 F)
非動作温度	- 25 ~ +70	- 25 ~ +70	- 25 ~ +70	- 25 ~ +70
動作湿度	95%相対湿度 (RH)	95%相対湿度 (RH)	95%相対湿度 (RH)	95%相対湿度 (RH)
動作高度	3,000m (9,843フィート) 25 (77 F)	3,000m (9,843フィート) 25 (77 F)	3,000m (9,843フィート) 25 (77 F)	3,000m (9,843フィート) 25 (77 F)
非動作高度	4,570m (15,000フィート) 25 (77 F)	4,570m (15,000フィート) 25 (77 F)	4,570m (15,000フィート) 25 (77 F)	4,570m (15,000フィート) 25 (77 F)
動作衝撃	1.88m/秒 (74インチ/秒) 1/2正弦入力	1.88m/秒 (74インチ/秒) 1/2正弦入力	1.88m/秒 (74インチ/秒) 1/2正弦入力	1.88m/秒 (74インチ/秒) 1/2正弦入力
非動作衝撃	60G 11ms1/2正弦入力	60G 11ms1/2正弦入力	60G 11ms1/2正弦入力	60G 11ms1/2正弦入力
動作振動	0.41Grms (5 ~ 500Hz) ランダム入力	0.41Grms (5 ~ 500Hz) ランダム入力	0.41Grms (5 ~ 500Hz) ランダム入力	0.41Grms (5 ~ 500Hz) ランダム入力
非動作振動	0.41Grms (5 ~ 500Hz) ランダム入力	0.41Grms (5 ~ 500Hz) ランダム入力	0.41 Grms (5 ~ 500Hz) ランダム入力	0.41Grms (5 ~ 500Hz) ランダム入力
熱放散 (最大電力使用時)	160.37BTU/時	160.37BTU/時	863.27BTU/時	863.27BTU/時
EMI	CE, VCCIクラスII, FCC, BCIQ, Austel	CE, VCCIクラスII, FCC, BCIQ, Austel	CE, VCCIクラスII, FCC, BCIQ, Austel	CE, VCCIクラスII, FCC, BCIQ, Austel
安全規格認定	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950
UL-1950標準	第3版	第3版	第3版	第3版
TUV EN 60950	第2版 Am.1-4	第2版 Am.1-4	第2版 Am.1-4	第2版 Am.1-4
EC-950/VDE-0805				
EN-60-950標準				
Bellcore	x	x	x	Bellcore GR-63およびGR-1089のテストで、NEBSレベル3に認定

¹ 00.5.12 フェールオーバーには、専用のシスコ製ケーブルが必要です。

ソフトウェアライセンスの選択

PIX 515(バージョン4.4)の場合、ライセンスは機能別となっています。すべてのPIX 515ソフトウェアは無制限のユーザーライセンスとともに提供され、ハードウェアにより制御される送信TCP/IPの同時接続の制限数は、ボックスごとに設定されています。

エントリレベルのPIX 515-R(制限付き)では、最大で50,000接続が可能です(PIX 515-Rはさらに制限があり、フェールオーバーが提供されず、10/100イーサネット・インタフェース数は2個に制限されています)。ミッドレンジのPIX 515-URでは、最大で100,000接続、フェールオーバー、最大で6個の10/100イーサネット・インタフェースが提供されます。

PIX 520の価格設定は、エントリレベル、ミッドレンジ、および無制限のライセンス提供とともに、今までと変わりません。PIX 520では、250,000以上の接続数、フェールオーバー、最大6個の10/100イーサネット・インタフェースが、最大4個のトークンリングまたは2個のFDDIインタフェースが提供されます。

NIC サポート

シングル・ポートの10/100BaseT Ethernet (PIX Firewall シャーシごとに最大4個のNIC PIX 515の制限付きソフトウェアではご利用できません)。

4ポートの10/100BaseT Ethernet(1つまたは複数のシングル・ポートの10/100BaseT Ethernet NICとの組み合わせが可能。ただし、PIX515の制限付きソフトウェアではご利用できません)。

4-/16-Mbpsのトークンリング(PIX Firewallシャーシごとに最大4個のNIC PIX 515ではご利用できません)。

FDDI(PIX FirewallシャーシごとにNICは2個まで。ただし、PIX515ではご利用できません)。

注意: シスコまたはシスコ認定の販売会社から購入したNICのみ、Cisco Secure PIX Firewall内でご使用いただけます。他のカードを使用すると、保証は無効となります。

TCP/IP プロトコルおよびアプリケーション・サポート

インターネット・プロトコル(IP)
 伝送制御プロトコル(TCP)
 ユーザー・データグラム・プロトコル(UDP)
 インターネット制御メッセージ・プロトコル(ICMP)
 GRE
 アドレス解決プロトコル(ARP)
 ドメイン・ネーム・システム(DNS)
 簡易ネットワーク管理プロトコル(SNMP)
 ブート・プロトコル
 ハイパーテキスト転送プロトコル(HTTP)
 ファイル転送プロトコル(FTP)
 トリピアル・ファイル転送プロトコル(TFTP)
 Archie
 Gopher
 Telnet
 NetBIOS over IP (Microsoft Networking)
 ポイントツーポイント・トンネリング・プロトコル(PPTP)
 SQL*Net (Oracleクライアント/サーバ・プロトコル)
 Network File System (NFS)などのSunリモート・プロシージャ・コール(RPC)サービス
 Berkeley Standard Distribution (BSD) -Rcmds
 AAAサーバ・グループ

マルチメディア・アプリケーション

Microsoft NetShow
 White Pine CU-SeeMe
 RealNetworks RealAudioおよびRealVideo
 Xing StreamWorks
 VDOnet VDOLive
 VXtreme WebTheater
 VocalTec Internet Phone

Videoconferencing (H.323) アプリケーション

Microsoft NetMeeting
 Intel Internet Video Phone
 White Pine Meeting Point

©2000 Cisco Systems, Inc. All rights reserved.

CiscoとCisco Systemsは商標です。CiscoのロゴはCisco Systems, Inc.の登録商標です。

この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。

本仕様は予告なしに変更される場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

E-mail: cnac@cisco.com

〒100-0005 東京都千代田区丸の内3-2-3 富士ビルヂング

TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先