VM-Series

VM-Series 次世代ファイアウォールの主な機能:

APP-ID™ によりすべてのアプリケーションをすべてのポートで常時識別

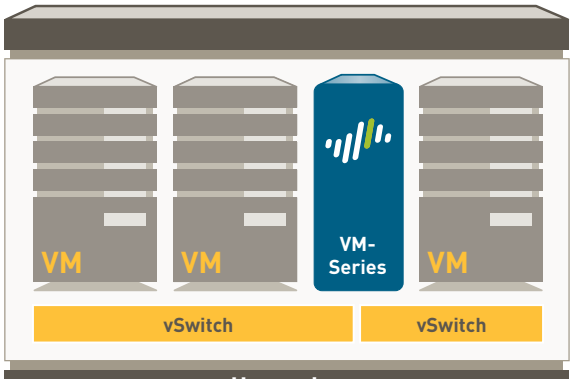
- 使用されているポートや暗号化（SSL または SSH）、セキュリティ回避技術に関わらず、アプリケーションを識別します。
- 許可、拒否、スケジュール、スキャン、帯域制御の適用などのセキュリティポリシー決定の要素として、ポートではなくアプリケーションを使用します。
- 不明なアプリケーションに、ポリシーコントロール、脅威のフォレンジック、カスタム App-ID の作成、またはApp-ID開発用のパケット キャプチャが行えるよう分類します。

USER-ID™ と GLOBALPROTECT™ であらゆる場所のあらゆるユーザに安全なアプリケーション使用ポリシーを拡張

- Active Directory、LDAP、eDirectory Citrix Microsoft Terminal Services とエージェントレスに統合します。
- NAC、ワイヤレス、その他の非標準のユーザ リポジトリを XML API に統合。.
- Microsoft Windows、Mac OS X、Linux、Android または iOS プラットフォームを実行しているユーザに一貫したポリシーを導入します。

CONTENT-ID™ と WILDFIRE™ で既知および未知のあらゆる脅威に対して保護

- 使用されている一般的な脅威回避技法が実装されているかに関係なく、すべてのポートでエクスプロイト、マルウェア、スパイウェアを含む様々な既知の脅威をブロックします。
- ファイルや機密データの無許可の転送を制限し、作業とは関係ない Web の利用を制御します。
- 未知のマルウェアを識別して、100 以上の悪意ある動作について分析を行い、自動的にシグネチャを作成して次の更新時に配信します。



VM-Series バーチャル ファイアウォール

Palo Alto Networks™ VM-Series は、安全なアプリケーション使用を仮想化された環境に拡張すると共に、ダイナミック アドレス オブジェクトを持つバーチャル マシンの移動の追跡、強力な XML管理 API を使用したオーケストレーション システムとの統合といった、仮想化に伴う主な課題に対処することができます。

VM-Series は VM-100、VM-200、VM-300 の 3 つの高パフォーマンスモデルで構成されています。シングル パス ソフトウェア構造により、データセンタ環境内の遅延を最小化します。管理プレーンとデータ プレーンは分離しており、ユーザがそれぞれに専用の CPU を割り当てることで、トラフィック の負荷とは無関係に常に管理アクセスを行うことができます。VM-Series の管理要素は、セキュリティに特化した専用のオペレーティング システム、PAN-OS™ で、これによって組織や企業は App-ID、User-ID、Content-ID、GlobalProtect および WildFire を使用してアプリケーションを安全に使用できます。

一般的な能力[1]	VM-300	VM-200	VM-100
最大セッション数	250,000	100,000	50,000
IPSec VPN トンネル/トンネル インターフェイス	2,000	500	25
GlobalProtect（SSL VPN）同時ユーザ	500	200	25
SSL 復号化セッション	1024	1024	1024
SSL インバウンド証明書	25	25	25
バーチャル ルータ	3	3	3
セキュリティ ゾーン	40	20	10
最大ポリシー数	5,000	2,000	250
アドレス オブジェクト	10,000	4,000	2,500
パフォーマンス1 および仮想化の仕様[1]			
ファイアウォール スループット（App-ID 対応）	1 Gbps		
脅威防御スループット	600 Mbps		
IPSec VPN スループット	250 Mbps		
新規セッション/秒	8,000		

[1] パフォーマンスと容量は、4 CPU コアを使用した最適なテスト条件のもと PAN-OS 5.0で測定されています。

paloalto NETWORKS
the network security company™

仮想化	VM-300	VM-200	VM-100
HyperVisor	VMware ESXi 4.1および ESXi 5.0		
ネットワーク ドライバ	VMXNet3		
CPU コア	2、4 または 8		
メモリ(最小)	4GB		
ディスク ドライブ容量(最小/最大)	40GB/2TB		

ネットワーキング

インターフェイス モード:

- L2、L3、タップ、バーチャル ワイヤ(トランスペアレント モード)

ルーティング

- モード: OSPF、RIP、BGP、スタティック
- フォワーディングテーブル サイズ(デバイス/VRごとのエントリ):
  5000/5000 [VM-300], 1250/1250 [VM-200], 1000/1000 [VM-100]
- ポリシーベースの転送
- マルチキャスト: PIM-SM、PIM-SSM、IGMP v1、v2、v3

高可用性(HA)

- モード: アクティブ/パッシブ、セッション同期なし
- 障害検出: パス モニタリング、インターフェイス モニタリング

アドレス割り当て

- デバイスのアドレス割り当て: DHCP クライアント/PPPoE/スタティック
- ユーザのアドレス割り当て: DHCP サーバー/DHCP リレー/スタティック

IPV6

- L2、L3、タップ、バーチャル ワイヤ(トランスペアレント モード)
- 機能: App-ID、User-ID、Content-ID、WildFire 、SSL 復号化

VLANS

- デバイス/インターフェースあたりの802.1q VLAN タグ: 4,094/4,094
- 最大インターフェイス数: 2000(VM-300)、500(VM-200)、100(VM-100)

NAT/PAT

- 最大 NAT ルール: 1,000(VM-300)、1,000(VM-200)、125(VM-100)
- 最大 NAT ルール(DIPP): 200(VM-300)、200(VM-200)、125(VM-100)
- ダイナミック IP およびポート プール: 254
- ダイナミック IP プール: 32,000
- NAT モード: 1:1 NAT、n:n NAT、m:n NAT
- DIPP オーバーサブスクリプション(一意の IP/ポートおよびIP):
  2 [VM-300], 1 [VM-200], 1 [VM-100]
- NAT64

バーチャル ワイヤ

- 最大バーチャル ワイヤ数: 1000(VM-300)、250(VM-200)、50(VM-100)
- バーチャル ワイヤにマップされたインターフェイス タイプ: 物理および
  サブインターフェイス

L2 転送

- ARP テーブル サイズ/デバイス: 2,500(VM-300)、500(VM-200)、500
  (VM-100)
- MAC テーブル サイズ/デバイス: 2,500(VM-300)、500(VM-200)、500
  (VM-100)
- IPv6 隣接テーブル サイズ: 2,500(VM-300)、500(VM-200)、500(VM-100)

セキュリティ

ファイアウォール

- アプリケーション、ユーザ、コンテンツに対するポリシーベースの制御
- 断片化されたパケットのプロテクション
- 偵察行為のスキャン プロテクション
- DoS（サービス妨害）//DDoS（分散サービス妨害）プロテクション
- 復号化: SSL（インバウンドおよびアウトバウンド）、SSH

WILDFIRE

- 100 以上の悪意ある動作について標的型および未知のファイルを識別し分析
- 新たに検出されたマルウェアに対してシグネチャを生成し自動的に配信
- 1 時間以内にWildFire シグネチャのアップデート配信、一体化されたロギングとれポーティんぐ、WildFire API で1 日あたり最大 100 サンプルのプログラム提出と、ファイル ハッシュによる 1 日あたり最大 1,000 レポートのクエリを実施可能（サブスクリプションが必要）

ファイルとデータのフィルタリング

- 1 ファイル転送: 60 以上の固有のファイルに対する双方向制御
- 1 データ転送: クレジットカード番号および米国社会保障番号の不正転送の双方向制御
- 1 ドライブバイ ダウンロード プロテクション

ユーザインテグレーション（USER-ID）

- Microsoft Active Directory、Novell eDirectory、Sun One およびその他の LDAP ベース ディレクトリ
- Microsoft Windows Server 2003/2008/2008r2、Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services、Citrix XenApp
- XML API による非標準ユーザ リポジトリとの統合助長

IPSEC VPN（サイト間）

- 鍵交換: 手動鍵、IKE v1
- 暗号化: 3DES、AES（128 ビット、192 ビット、256 ビット）
- 認証: MD5、SHA-1、SHA-256、SHA-384、SHA-512
- 動的 VPN トンネル作成（GlobalProtect）

脅威防御（サブスクリプションが必要）

- アプリケーション、オペレーティング システムの脆弱性エクスプロイトの防御
- ストリームベースのウイルス防御（HTML、Javascript、PDF への組み込み、圧縮形式のものを含む）、スパイウェア、ワーム

URL フィルタリング（サブスクリプションが必要）

- 事前定義済みおよびカスタム URL カテゴリ
- 最近アクセスした URL のデバイス キャッシュ
- セキュリティ ポリシーの一致条件としての URL カテゴリ
- 閲覧時間の情報

サービス品質（QOS）

- アプリケーション、ユーザ、送信元、宛先、インターフェイス、IPSec VPN トンネル、その他多数のエレメントごとのポリシーベース　トラフィック シェーピング
- 保証、最大、優先帯域幅パラメータを備えた 8 つのトラフィック クラス
- リアルタイム帯域幅モニタ
- ポリシーごとの diffserv マーキング
- QoS でサポートされている物理インターフェイス: 6（VM-300、VM-200）、4（VM-100）

SSL VPN/リモート アクセス（GLOBALPROTECT）

- GlobalProtect Gateway
- GlobalProtect Portal
- トランスポート: SSL フォールバックを伴う IPSec
- 認証: LDAP、SecurID、ローカル DB
- クライアント OS: Mac OS X 10.6、10.7（32/64 ビット）、10.8（32/64 ビット）、Windows XP、Windows Vista（32/64 ビット）、Windows 7（32/64 ビット）
- サード パーティのクライアント サポート: Apple iOS、Android 4.0 以上、Linux用VPNC IPSec

管理、レポート、可視性ツール

- 統合Web インターフェイス、CLI、集中管理（Panorama）
- マルチ言語のユーザ インターフェイス
- Syslog、Netflow v9、SNMP v2/v3
- XML ベースの REST API
- アプリケーション、URL カテゴリ、脅威およびデータのグラフィカル サマリ（ACC）
- トラフィック、脅威、WildFire、URL、データ フィルタリングの各 ログの閲覧、フィルタ、エクスポート
- 完全にカスタマイズ可能なレポート機能

VM-Series 次世代ファイアウォールの詳細は、www.paloaltonetworks.com/literature を参照してください。

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com