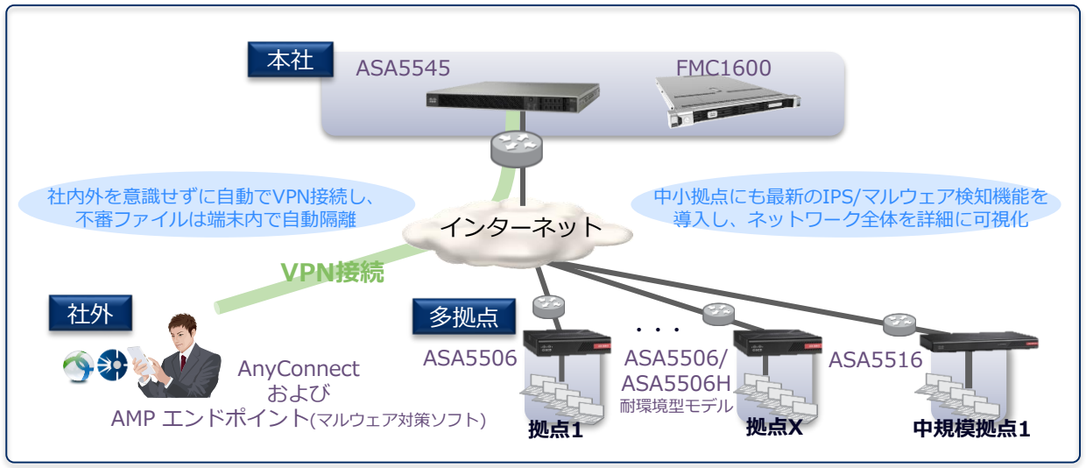
利用例

- 多拠点を専用管理製品「Firepower Management Center」で一括管理と相関分析可能。
- 社外でのWebアクセスも自動VPN接続でASAを経由させ、社内ポリシーの管理下に。



仕様一覧

製品モデル		ASA5506	ASA5508	ASA5516	ASA5525	ASA5545	ASA5555
製品写真							
スループット	Firewall	750Mbps	1Gbps	1.8Gbps	2Gbps	3Gbps	4Gbps
	VPN	100Mbps	175Mbps	250Mbps	300Mbps	400Mbps	700Mbps
	Firepower	250Mbps	450Mbps	850Mbps	1.1Gbps	1.5Gbps	1.75Gbps
最大VPNクライアント数		50	100	300	750	2,500	5,000
同時セッション数		50,000	100,000	250,000	500,000	750,000	1,000,000
1秒あたりの新規セッション数		5,000	10,000	20,000	20,000	30,000	50,000
VLAN数		30	50	100	200	300	500
仮想FW数		–	5	5	20	50	100
冗長構成	Failover機能	○					
	二重化電源	–				○	
耐環境性能		○	–				

管理製品	FMC仮想版	FMC1600	FMC2600	FMC4600
製品写真	–			
管理デバイス数	2 / 10 / 25	50	300	750

冗長機能等の一部機能は各種モジュール搭載およびライセンス適用時です。また一部併用できない機能があります。
ASA5506はセキュリティプラスライセンス利用時の値です。

安全に関するご注意	★本製品の設置/接続/使用に際しましては、取扱説明書などに記載されております注意事項や禁止事項を熟読のうえ、必ずお守り下さい。

お問い合わせは、下記のNECへ
デジタルネットワーク事業部
URL：https://jpn.nec.com/datanet/cisco/

Specialization
- Advanced Service Provider Architecture Specialization
- Advanced Data Center Architecture Specialization
- Advanced Enterprise Networks Architecture Specialization
- Advanced Security Architecture Specialization

日本電気株式会社 〒108－8001 東京都港区芝五丁目7－1(NEC本社ビル)　2019年10月現在　Ver.12　20191021BCC221

Orchestrating a brighter world　NEC

次世代ファイアウォール/IPS

Cisco ASA5500シリーズ

ファイアウォール/VPN/IPS/マルウェア解析など多彩な機能を搭載
ネットワーク全体をカバーするオールラウンドのセキュリティ製品

グローバルで実績と定評のある数々のセキュリティ機能を一台に凝縮。
世界最大の解析力を持つセキュリティ基盤と連携し、最新の脅威に即座に対応します。

多層防御をすり抜けるサイバー攻撃に対抗する総合セキュリティ対策

- **求められるのは問題発生時の迅速な対応**
  近年、高度なマルウェアにより、情報流出などの被害が拡大しています。これらに対し、単一のセキュリティフェーズや製品だけで全ての脅威に対処することは不可能であり、感染発覚時の事後対策が必須です。

<セキュリティ対策の流れ>

侵入	検出	復旧
●次世代ファイアウォール ●VPN	● IDS/IPS ●ボットネット対策	●マルウェア防御/解析および感染経路と原因の特定

シスコセキュリティは従来から重視されている侵入/検出フェーズだけでなく、問題発生時の原因特定と障害復旧および再発防止を迅速に行い、短期間での復旧を実現します。

ASA Firepowerシリーズが提供する脅威対策

- **次世代FW/IPSとしての高度な検知と分析力に加え、管理面でも充実した機能を提供します。**

★管理製品Firepower Management Center利用時の機能

業界最高水準のIPSエンジン

[IDS/IPSとして実績No,1のエンジン"Snort"を採用]

すでに世界で30万以上がセンサーとして稼働中であるIPS業界の標準コアエンジンです。

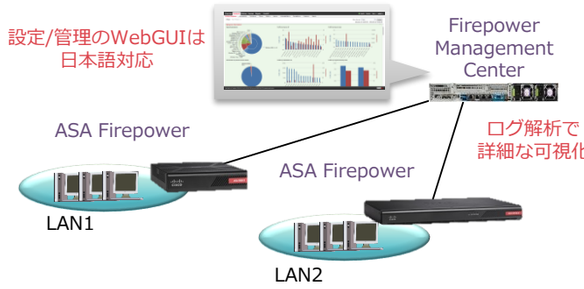
検知率評価NO,1
総シグネチャ数3万以上
Windowsゼロデイ脆弱性カバー率NO,1

検知率は全モデルで同等です。
オープンソースであるため検知要因を管理者が明確に把握することができます。

ネットワークとホストの可視化/管理

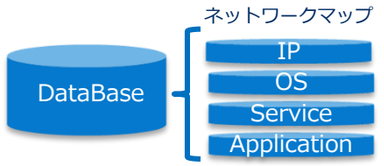
[設定/ログ解析ツール]

FirepowerはFirepower Management Centerで管理します。
複数の機器から情報を収集し、相関分析が行えます。



[ネットワークマップの作成]★

監視対象ネットワーク上のホスト情報を収集し、全てをまとめたマップを作成します。



ネットワークマップでホストごとにOSや使用アプリなどの詳細情報が可視化できます。また、収集した情報はイベント解析などに利用されます。

次世代ファイアウォール機能

[URLフィルタ機能]

指定したURLやカテゴリ(SNS/ゲーム/ビデオなど)ごとにWebアクセスを制御できます。

[アプリケーション制御]

通信をモニタし、アプリケーションを識別することで、個別またはカテゴリごとに動作の制御が可能です。

従来のファイアウォールより柔軟な制御が行えます。

アプリ内の動作も制御可能

かんたん設定

[推奨設定]

初期設定は「防御優先」「バランス重視」「通信優先」の推奨設定から一つを選択するだけで完了します。

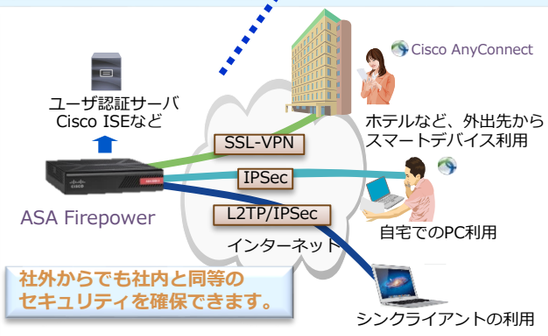
複雑な初期設定が容易に行えます。

[IPSシグネチャ自動チューニング]★

ネットワーク環境を学習し、推奨設定を自動でチューニングするので常に最適な環境で利用できます。

必要なシグネチャのみ有効化されるので誤検知が大幅に削減できます。

数種のVPNの同時収容

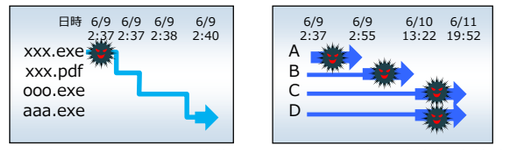


社外からでも社内と同等のセキュリティを確保できます。

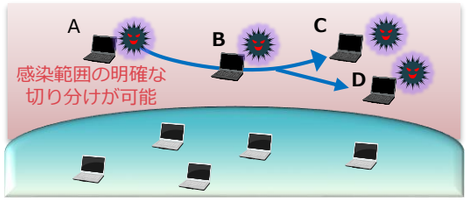
SSL-VPN、IPSec、L2TP/IPSecを同時に利用できるため、異なるデバイスによる自由度の高いVPN構成が実現可能です。

感染範囲を一目で判断

[ファイル追跡]★



一度検査に通ったファイルでも挙動を把握しておくため、後にマルウェアだと判明した場合、即座に隔離することが可能です。また、感染が発覚した場合、影響を受けた端末や経路を特定し、感染範囲を最小限に抑えます。



万一の感染時に原因の究明、障害復旧、再発防止が迅速に行えます。

※マルウェア検知は単体のみで動作可能(管理製品不要)
※端末内の挙動確認には別途クライアントソフトが必要