



最先端のFirewall新機能紹介

- あなたのセキュリティを次のレベルへ

中村 光宏, GSSO Sr. SE Manager
中村 太亮, CX Customer Success Specialist

シスコシステムズ合同会社

October, 2024

Agenda

- 1 現在求められるFirewallの姿
 - 1.1. 次世代FWとは
 - 1.2. Cisco Firewallのビジョン
 - 1.3. Cisco Firewall 新H/W + AI
- 2 FTD魅力ある新機能&保守運用効率化
4選 紹介
- 3 まとめ と Q&A

Firewallの歴史変遷：いつまで次世代??

第一世代

パケットヘッダーで通信を制御

1990s~

当時のプレイヤー

Checkpoint Firewall 1

第二世代

- ・ アプリ可視化と他のセキュリティ機能を搭載したUTM

2000s~

当時のプレイヤー

Cisco PIX / ASA

Netscreen

第三世代=次世代(NGFW)

- ・ アプリ、ユーザー、コンテンツに基づくより深い可視化と制御
- ・ SSL/TLS復号技術により、機密情報も解読可能に

2008~

当時のプレイヤー

Palo Alto PAシリーズ



次世代と呼ばれて16年が経過...

* <https://www.paloaltonetworks.com/cyberpedia/the-evolution-of-firewalls-from-packet-filtering-to-machine-learning-powered-ngfws>

“

その次世代Firewall
もう時代遅れなのでは？

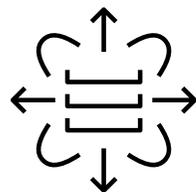


過去から価値が低下している・・・「旧・次世代Firewall」



暗号化(HTTPS)通信が増え
脅威検知が困難化

暗号化通信を復号し検査・対策しようにも
処理性能減や通信影響リスク、運用複雑化など課題山積



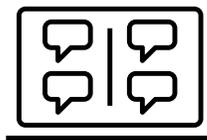
増え続ける通信に
高速化対応が必要

世界平均で毎年 20% 通信量の増加(シスコ調査)
Firewall 台数を増やそうにも、予算や設置場所の制約



日々 ACLが溜まっていき
管理負荷が増大

担当者代々で日々たまるACLなど設定を整理しようにも
その時間の確保が難しく、設定が膨らみ続ける悪循環



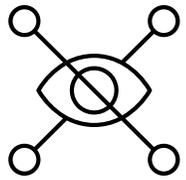
オンプレとマルチクラウドとの
分散管理による負担増で
セキュリティ低下

各製品で管理GUIや設定方法が異なり、ログも分散
設定管理の負荷増大や セキュリティイベント見逃しリスク増



市場の相対価値は下がり、機能・運用の懸念に加え、過去からの**値上げ**もあってコスト増も悩みの種に

Cisco Secure Firewallによる次世代化のご提案



暗号可視化エンジン **EVE**

暗号化された“まま”で、ラクラク脅威遮断
HTTPS/3やQUICも対応、次世代エンジン



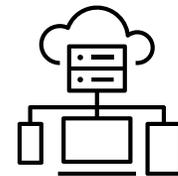
高速化対応で 卓越した **ROI**

1RUで 業界トップクラスの 140Gbps (FW+AVC+IPS)
最大 16台のクラスタ Active-Active 構成も可能(最新機種)



ACLなどポリシー最適化 **AI** が支援

長期未使用ACLや重複ポリシーの検知・通知や無効化支援
設定やトラブル時の解決支援も AIにお任せ



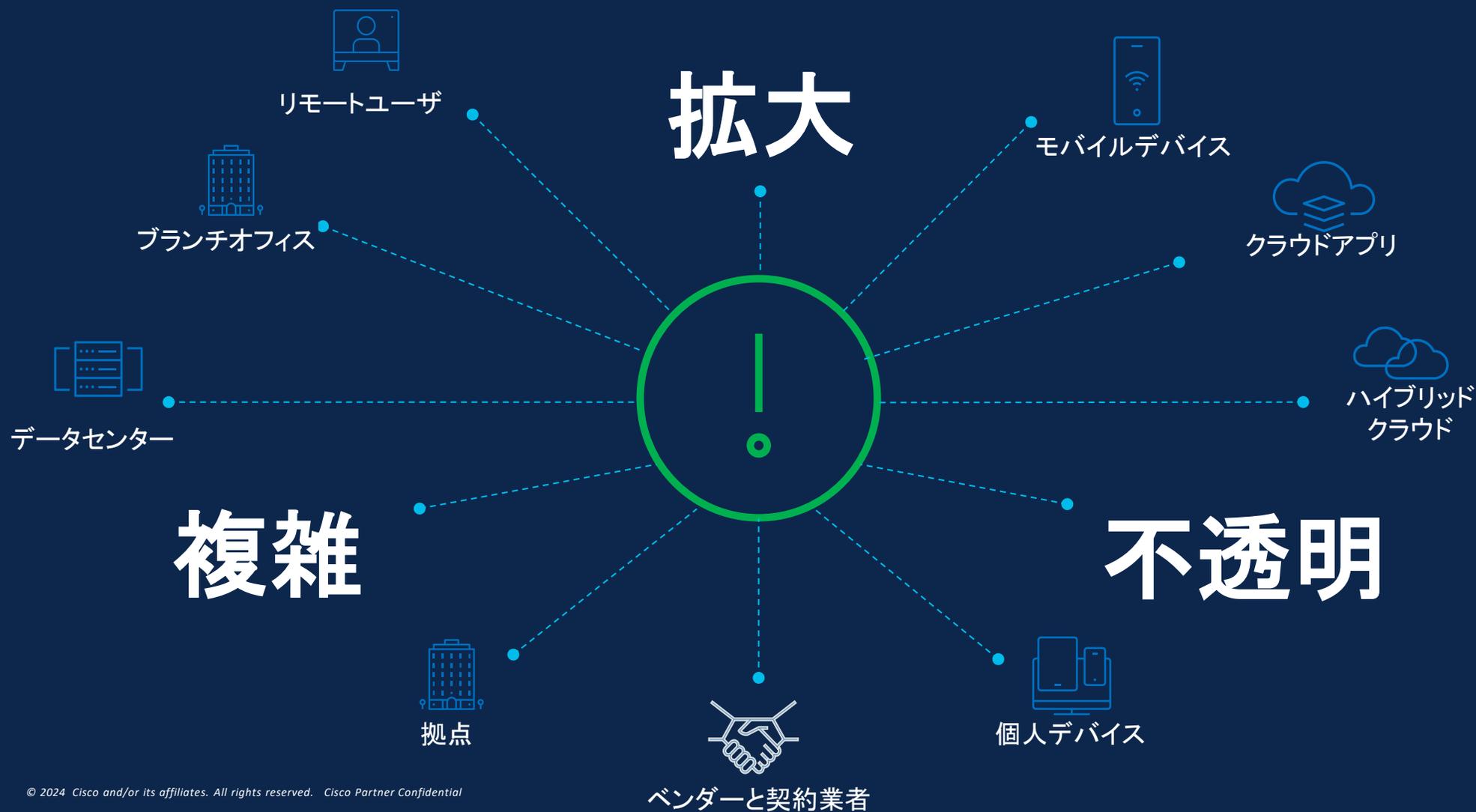
オンプレもマルチクラウドも 簡単に**一元管理**

オンプレや AWS・Azure・Google Cloud を統合管理・連携し脅威
検知と封じ込めが可能。クラウドネイティブで導入展開も楽



期間限定で乗換特典をご用意しています！

ネットワークの攻撃サーフェスはますます拡大している...



ユーザは、次のようなものを求めている

今の時代に有効なNGFWは変化しています



完全な可視化

多様なアタックサーフェスとセキュリティコンプライアンスの状態



包括的な脅威対策

ネットワークトラフィックの増加やビジネスニーズに合わせて拡張できる



容易な設定と管理

ハイブリッドクラウドとオンプレミスネットワークの運用

Cisco Secure Firewall -新しい時代のファイアウォール

- Apps
- Users

攻撃対象の完全な可視化

- Devices
- Clouds

業界をリードする
intrusion prevention,
Snort3

業界で最初の
Encrypted Visibility Engine

世界最大規模の脅威インテリ
ジェンス組織
Talos

業界最新生成AIによる
Cisco AI Assistant

- Malware
- 既存の脆弱性
- 危険な URL
- DNS
- Web ベースの攻撃

包括的な脅威対策



- Cloud / on-prem / on-box の
管理オプション
- ロータッチプロビジョニング
- フレキシブルな消費モデル

容易な設定と管理

包括的な機能を備えたシスコのファイアウォール

優れた脅威からの保護

Cisco Talos セキュリティ インテリジェンス



アプリケーション
制御、カスタム
アプリディテクタ



侵入防御



自動化、修復、
統合



マルウェア防御
とサンドボックス
分析



URL フィルタリ
ングおよび分類



ファイアウォール、
ルーティング、
NAT



高可用性および
高拡張性



VPN/ZTNA



TLS 復号



ML 主導の
暗号化された
可視化エンジン



ID および属性
ベースの
アクセス制御

設定および分析コンソール

将来を見据えたプラットフォーム

他のどのベンダーよりも多くのフォームファクタに対応

統合管理

XDR

Talos



Cisco
Secure Firewall
ハードウェア



Cisco
Secure Firewall
仮想およびコンテナ化



Cisco
Umbrella
クラウド提供型
ファイアウォール



Cisco
Multicloud Defense
マルチクラウド



Cisco
Secure Firewall
as-a-service

ユースケース

ZTNA/VPN

SASE

IoT/IIoT/OT

アプリケーション
セキュリティ

データセンター/境界

マルチクラウド

通信事業者と
サービスプロバイダー

ゼロトラスト マイクロ
セグメンテーション

可視化

包括的な脅威対策

容易な設定と管理

Agenda

- 1 現在求められるFirewallの姿
 - 1.1. 次世代FWとは
 - 1.2. Cisco Firewallのビジョン**
 - 1.3. Cisco Firewall 新H/W + AI
- 2 FTD魅力ある新機能&保守運用効率化
4選 紹介
- 3 まとめ と Q&A

複雑さがセキュリティの盲点を生む

複雑な
ルール

010110
110010
001011

設定ミス



スキルセット
の需要



脆弱なセキュリティ態勢

アウテージ/ダウンタイム

リアクティブプロセス

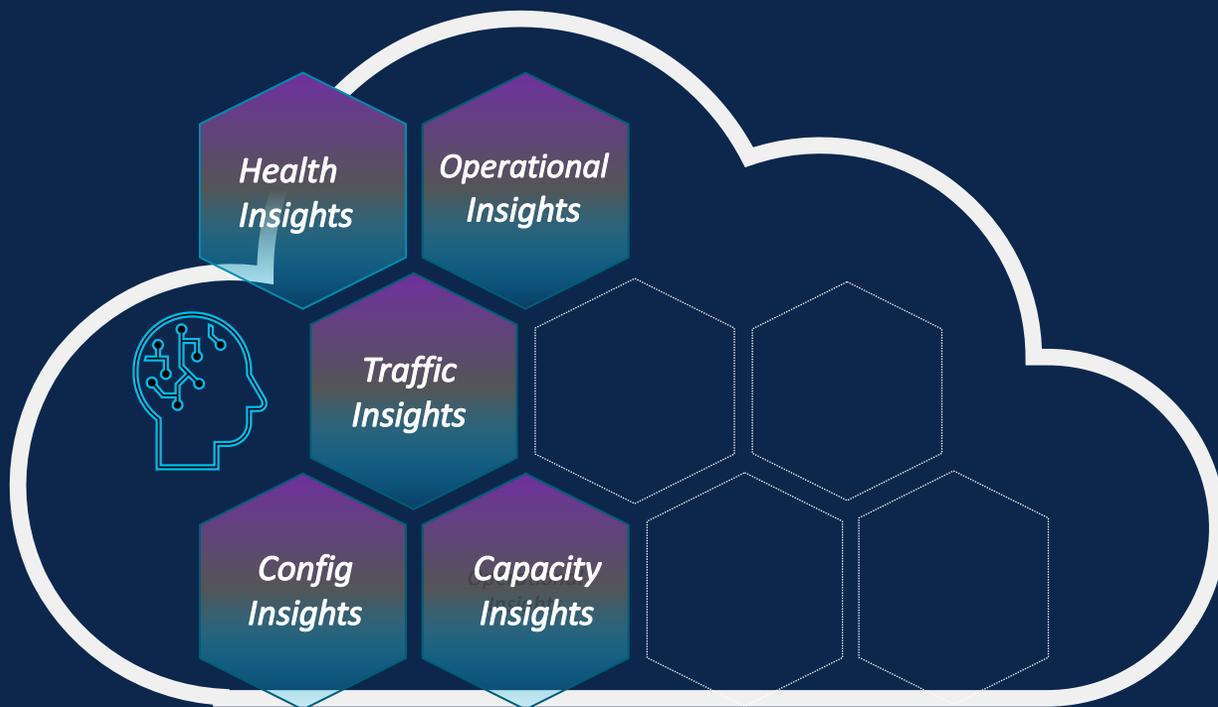


ネットワーク・ダウンタイムの平均コストは1時間当たり30万ドル



AIOps Vision

Ciscoファイアウォールの運用の簡素化とセキュリティ態勢の強化



- ベストプラクティスを推奨することで、設定ミスを防ぎ、セキュリティ体制を強化する
- 予測分析とダイナミック・ベースラインを使用して、根本原因の分析とパターンの予測/予測を行う
- ServiceNowのような変更管理システムとの統合を含む、処方的およびガイド付きの改善策を受け取る
- 簡単なポリシー管理と最適なファイアウォール性能を実現するために、お客様の環境に合わせたポリシーの最適化提案と改善策を届ける
- シスコAIアシスタントとのシームレスなインタラクションを体験し、人間の業務を支援・補強する

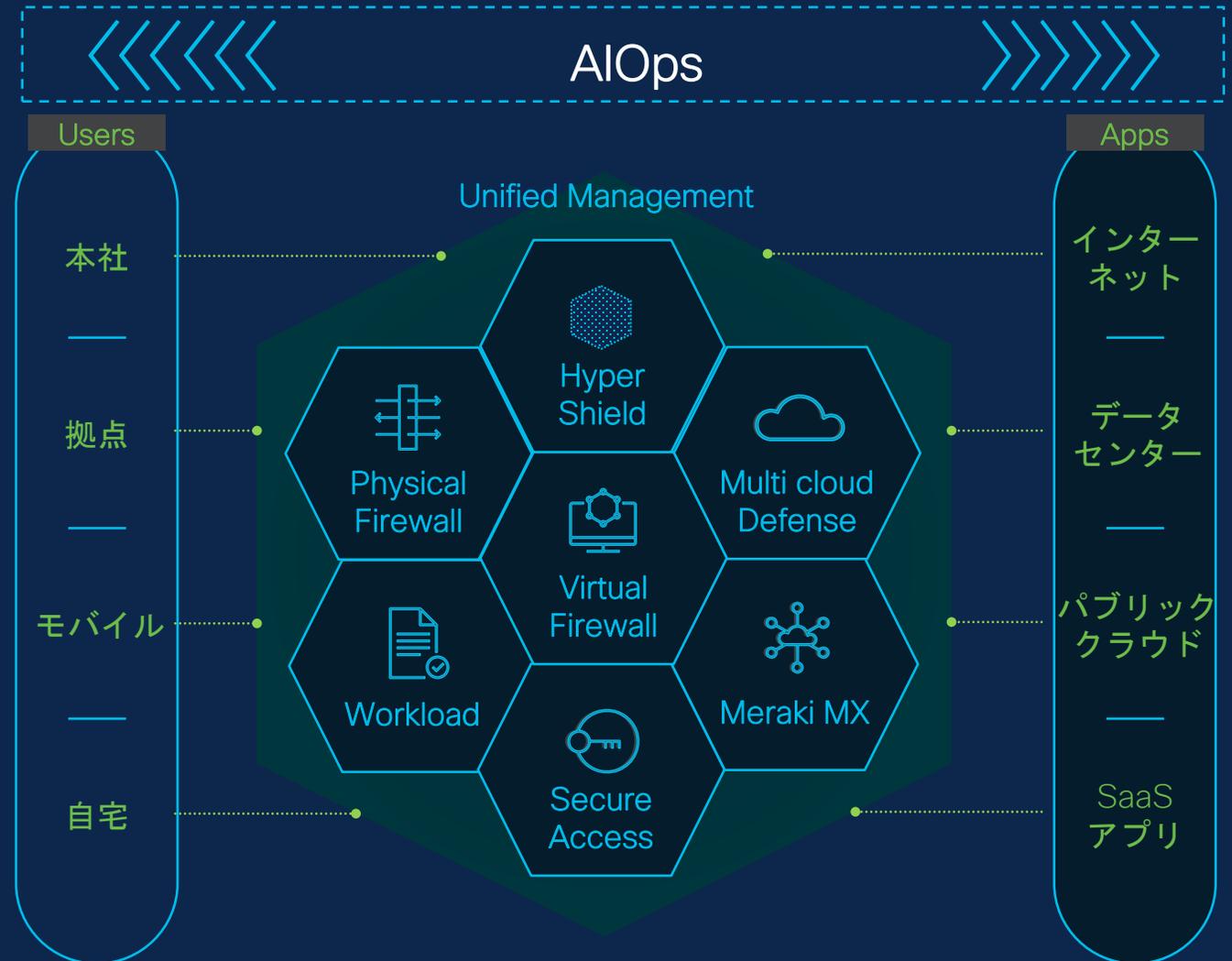
デバイスごとに1日あたり300万件のメトリクスからインサイトを導き出す

Logs, Events, Metrics, Telemetry, Configuration, Database, Traces

Unified Security Management Vision

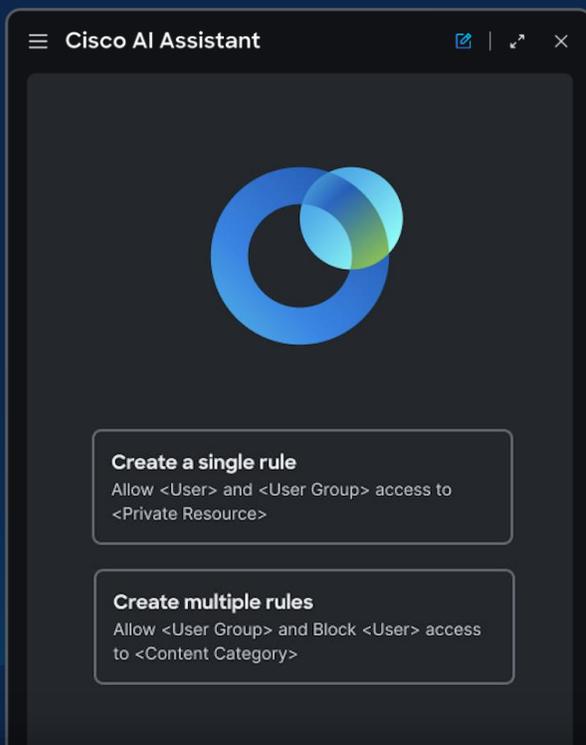
For Hybrid Mesh Firewall

サービスとしてのAIOpsは、人工知能と機械学習のパワーを活用し、運用上の洞察を活用してセキュリティ態勢を強化し、ハイブリッド・メッシュ・ファイアウォール・エコシステムをプロアクティブに強化する



Gartner definition of [AIOps](#)

← セキュリティのためのシスコAIアシスタント →



Cisco AI Assistant

How do I schedule a recurring backup?

To schedule a recurring backup, follow the steps below:

1. In the Frequency field, select daily, weekly, or monthly backup.
2. Select the time of day, in 24-hour time, you want the backup to occur. Note that you schedule the time in Coordinated Universal Time (UTC).
 - For weekly backups: Check the days of the week on which you want the backup to occur.
 - For monthly backups: Click in the Days of Month field and add whichever days of the month you want to the schedule the backup. Note: If you enter day 31 but a month doesn't have 31 days in it, the backup will not take place.
3. Give the scheduled backup time a name and a description.
4. Click Save.

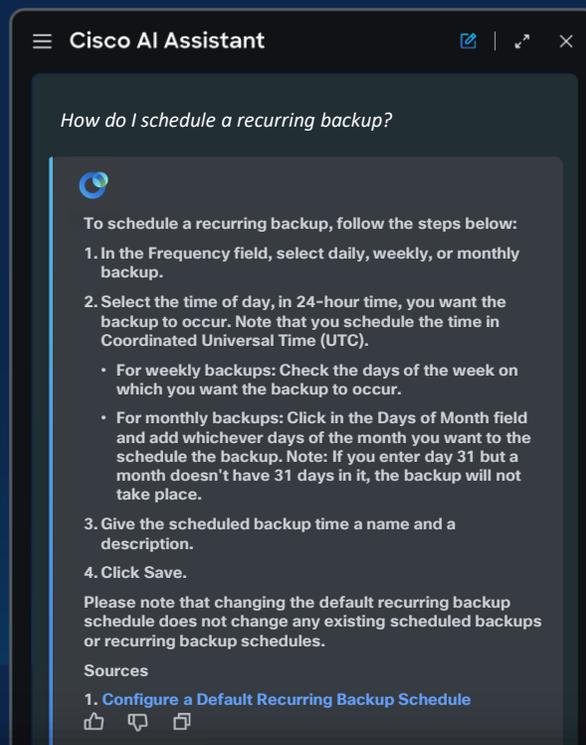
Please note that changing the default recurring backup schedule does not change any existing scheduled backups or recurring backup schedules.

Sources

1. [Configure a Default Recurring Backup Schedule](#)

Create a single rule
Allow <User> and <User Group> access to <Private Resource>

Create multiple rules
Allow <User Group> and Block <User> access to <Content Category>



Cisco AI Assistant

The **Close Incident** action is in progress. You can check on the status of this action by viewing it in [Workflow](#).

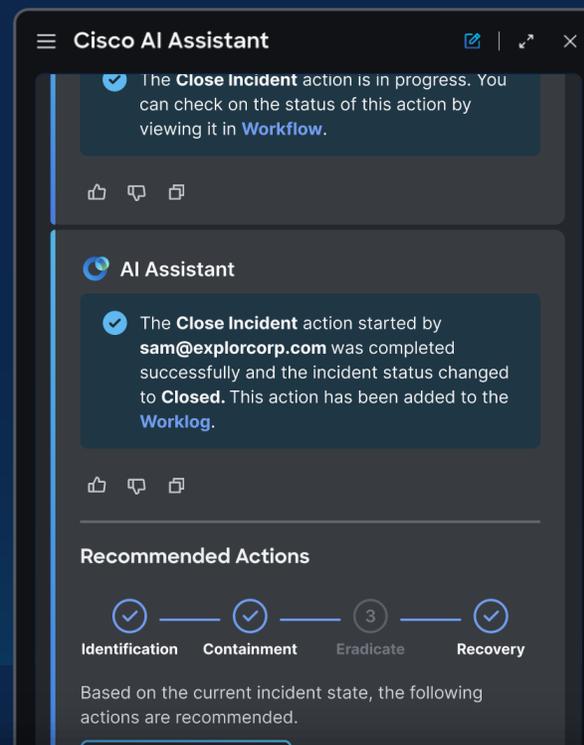
AI Assistant

The **Close Incident** action started by [sam@explorcorp.com](#) was completed successfully and the incident status changed to **Closed**. This action has been added to the [Worklog](#).

Recommended Actions

Identification — Containment — 3 — Recovery

Based on the current incident state, the following actions are recommended.



Cisco AI Assistant

Prove the Distributed Exploit Shield is working

This Distributed Exploit Shield will block **httpd** from executing a script in **/tmp**, thereby precluding remote code execution.

We've tested this in the shadow dataplane and no deviations within the thresholds were found.

[View test results](#)

Are there public exploits available for the CVE?

[View More](#)

Ask a question

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

Secure Access

ファイアウォール

XDR

Hypershield

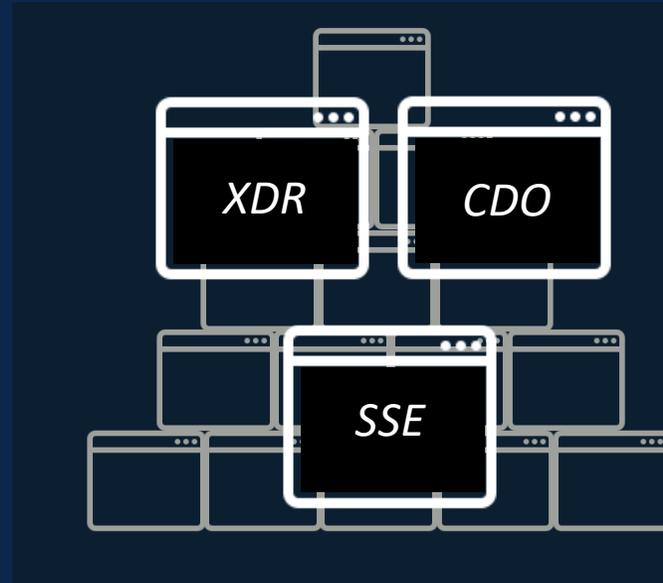
Security Cloud Control: Common Management

Historically



20+ Product Consoles

Today



Platform Experiences are emerging...

defenseorchestrator.com
xdr.cisco.com
sse.cisco.com

この最後の飛躍を
どうするか？



Security
Cloud Control



Unified management

security.cisco.com

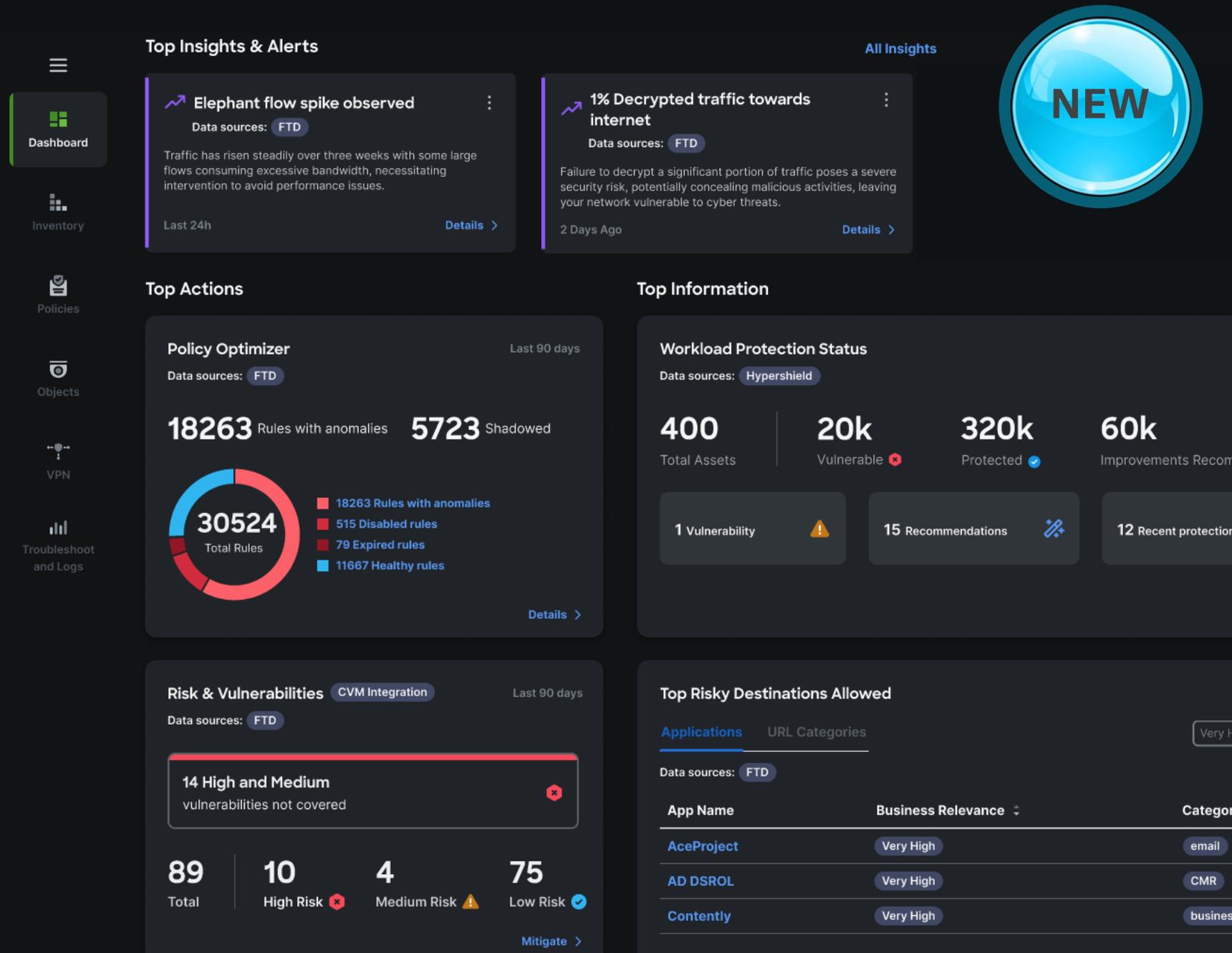
Security Cloud Control

AIの活用

ルール、ポリシー、設定の最適化
重複や設定ミスの検出

エレファント・フローのような異常の検出

ハイブリッド・メッシュでSASE
体感品質の向上



Agenda

- 1 現在求められるFirewallの姿
 - 1.1. 次世代FWとは
 - 1.2. Cisco Firewallのビジョン
 - 1.3. Cisco Firewall 新H/W + AI**
- 2 FTD魅力ある新機能&保守運用効率化
4選 紹介
- 3 まとめ と Q&A

Cisco Secure Firewall のハードウェア更新

脅威の状況が進化するにつれて、シスコのファイアウォールポートフォリオも進化。同価格以下のコストでさらに機能が追加され、パフォーマンスが向上



パフォーマンスの向上

- ファイアウォール スループットが最大 3.5 倍向上
- VPN スループットが最大 5 倍向上



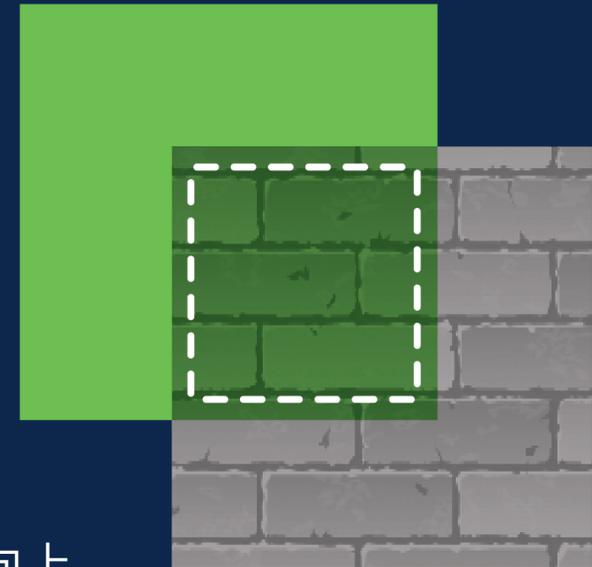
接続性の強化

- 1 秒あたり最大 2 倍の接続数 (CPS)

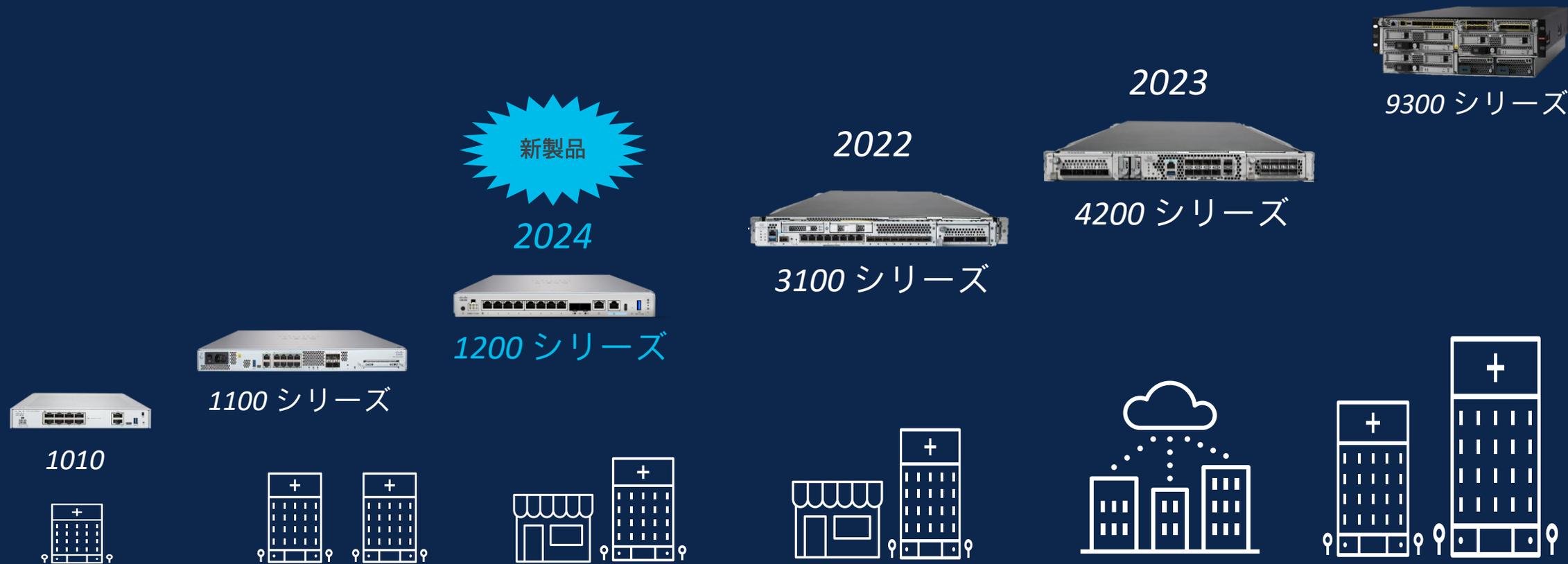


暗号化されたトラフィックのスループット向上

- 暗号化されたトラフィックのパフォーマンスが最大 3 倍向上



Cisco Secure Firewall ハードウェアポートフォリオ



Cisco Secure Firewall 4200 シリーズ



ソフトウェアは **FTD** と **ASA** の選択が可能

優れたパフォーマンス

- 強力なハードウェア、幅広い高速ネットワーク インターフェイス、1 RU のフットプリントで、優れたパフォーマンスの packets 処理を実現
- TLS と IPsec の復号を加速する暗号化アクセラレーション対応のアーキテクチャにより、暗号化トラフィックを可視化

卓越した ROI

- 最大 16 台のファイアウォールデバイスにまで拡張できるクラスタリング機能を備えているため、ビジネスの成長に合わせてセキュリティ インフラストラクチャを拡張可能
- Fail-to-Wire インターフェイスをはじめ、ホットスワップ対応ネットワークモジュールを使用して、ビジネス稼働時間を維持することが可能

1RU、16 台のクラスタ構成が可能、200G インターフェイスのサポート、インターフェイス モジュール ベイ X2、デュアル SSD、デュアル管理インターフェイス

Cisco Secure Firewall 3100 シリーズ

- 高性能 ミッドレンジアプライアンス
- 脅威に重点を置いたセキュリティアーキテクチャ
- 柔軟な導入オプション：
 - ファイアウォール
 - 専用の侵入防御システム
 - マルチインスタンスのサポート
 - 最大 8 台のアプライアンスをクラスタ化

価格性能比に優れた、大規模企業およびデータセンター向けセキュリティ



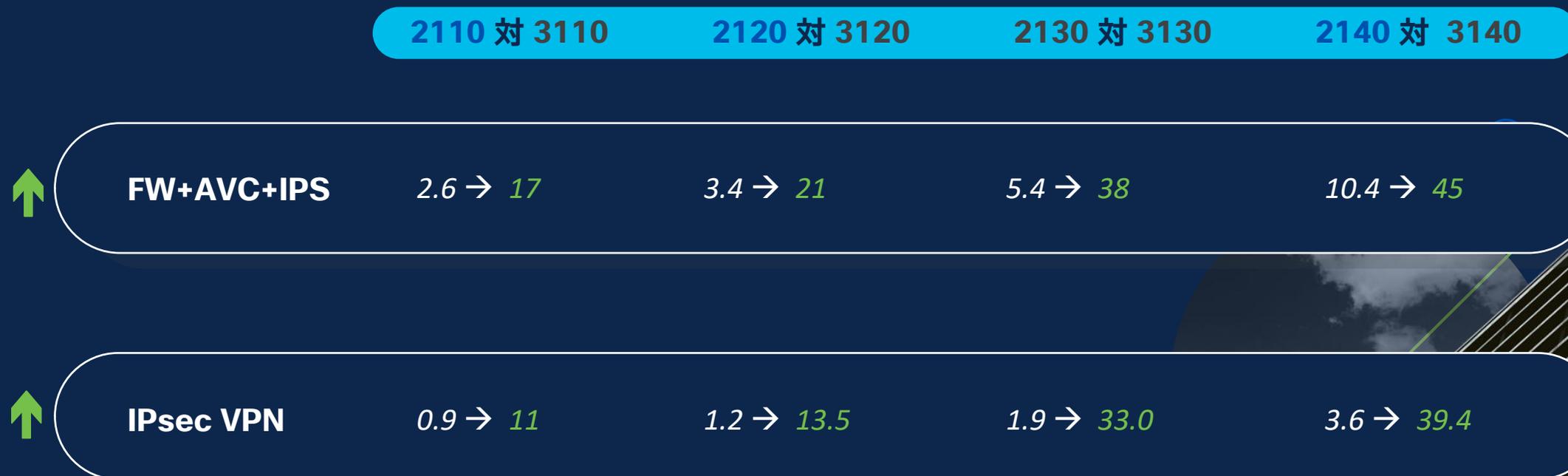
5つのアプライアンスモデル：
3105、3130、3120、3130、3140
ファイアウォール スループット：
最大 **45 Gbps***

ソフトウェアは FTD と ASA の選択が可能

* 1024B FW+AVC+IPS

最大 3 倍のパフォーマンス

Secure Firewall 2100 シリーズと Firepower 3100 の比較



*パフォーマンスの推定値は **Gbps** 単位、パケットサイズは **1024** バイト。プロトコルタイプなどのネットワーク要因によって異なります。

Firepower 3100 シリーズの **IPSEC** の数値は、**VPN オフロードを有効にした場合のもので**す。

Cisco Secure Firewall 1200C シリーズ

FTD
7.6

ASA
9.22

分散型エンタープライズブランチ向けの最高性能の SD-WAN 対応コンパクトファイアウォール

↑ 3 倍以上
他を上回る
性能

↑ 2 倍以上
他を上回る
価格性能比



コンパクトな設置面積で
優れた性能を実現

展開を効率化、HW の
追加が不要

AI/ML ベースの検出と管理

Cisco Secure Firewall 1200C シリーズ

分散型エンタープライズブランチ向けの最高性能の SD-WAN 対応コンパクトファイアウォール。

コンパクトな設置面積で優れた性能を実現

- 本社やクラウドアプリケーションへの接続速度が3倍になり、従業員の生産性が向上します。
- UPoE+ で IoT デバイスに直接電力を供給したり、SFP+ ポートでデスクトップファイアウォールの性能を向上させたりできます。

展開を効率化、HW の追加が不要

- 組み込みのオンボーディングテンプレートとゼロタッチプロビジョニングにより、複数のブランチ拠点に SD-WAN を迅速に展開できます。
- ブランチで複数のネットワークングデバイスを購入、展開、管理する必要がなくなります。

AI/ML ベースの検出と管理

- AI/ML を活用し、暗号化されたマルウェア、一般的な脅威、ゼロデイ脆弱性を検出します。
- AI Assistant が、オンプレミスまたはクラウド向けのファイアウォールの運用とポリシーのライフサイクル管理を合理化します。

Cisco Secure Firewall 1200C シリーズ

1220 CX

1G または 10G SFP+ X 2
6 Gbps

1210 CP

UPoE+ X 4
3 Gbps

1210 CE

3 Gbps

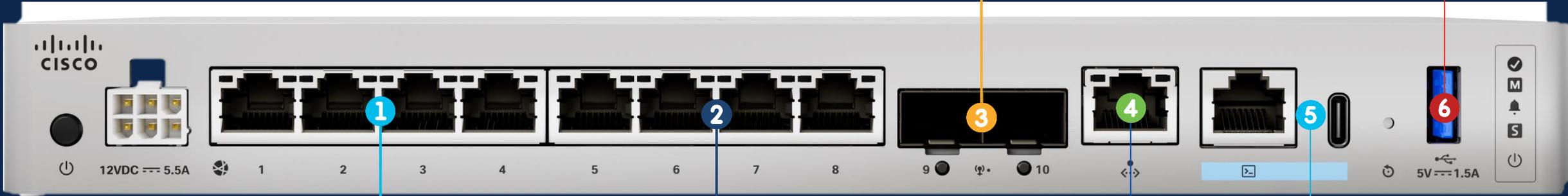


Cisco Secure Firewall 1200C シリーズ

Desktop form factor; optional rack mounting kit
Quiet blower for active cooling
External brick-style AC power adapter

2x SFP+
on CSF1220CX model

USB 3
Type A



8x 1000BASE-T
Ethernet

4 ports with UPoE+
on CSF1210CP model

Management
Ethernet

RJ-45 & USB-C
console

Firewallを使っているお客様の課題

-  ポリシー/ルールセット/機能が複雑で大量にあるため、設定不備が発生し、セキュリティ、有効性、効率性が低下
-  大量のドキュメントとトラブルシューティングのリポジトリが複数個所に分散しているため、コンテキストのない状態での検索と実装の作業が増加
-  監査レポートとコンプライアンスレポートの要件が増大しているため、調査とレポート作成作業も増大
-  セキュリティ担当者の離職率の高さとその急上昇、および熟練労働者の不足により、新任管理者による習得が極めて困難

AI アシスタント

お客様からのフィードバックに基づくユースケース

セキュリティの
向上



設定不備の解消により、正確性とパフォーマンスが向上

可視性の向上



監査、コンプライアンス、レポート作成のための、ポリシーやアクセス権の調査がスピードアップ

運用効率の向上



ドキュメントやトラブルシューティングの情報源から、シスコが認定した情報、対応、ベストプラクティスを特定し、コンテキストに応じた対応を実施

迅速なアクション



ユーザーインターフェイス内での迅速で直感的なアクションを通じて、習得期間を短縮し、スキルギャップを克服

Cisco AI Assistant for Security

cdFMC

Return to Access Control Policy

ACP - Production

Analyze Rule Heartbeat Reset Save

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More Targeted: 3 device

Search Total 9 rules Add Category Add Rule Ask AI

Name	Action	Source				Destination			
		Zones	Networks	Ports	Dynamic Attributes	Zones	Networks	Ports	Applications
Mandatory									
There are no rules in this section Add Rule or Add Category									
Default (1-9)									
<input type="checkbox"/> 1 External	Block	Any	any-ipv4 -1 more	Any	Any	Any	Any	TCP_47001	Any
<input type="checkbox"/> 2 Internal	Allow	Any	any -1 more	Any	Any	Any	Any	TCP_8302	Cisco
<input type="checkbox"/> 3 Block Malwares	Block	Any	any-ipv4 -1 more	Any	Any	Any	Any	Any	Tinych
<input type="checkbox"/> 4 Block Torrent	Block	Any	Germany -8 more	Any	Any	Any	Any	Bit-torrent	Torren

Default Action: Intrusion Prevention: Balanced Security and Con...

Ask Cisco AI

Show me access policies related to the user group Imm-vendor

Cisco Assistant 8:12 AM

Absolutely! There are 3 Access Control Policies related to user group Imm-vendor. There are 10 Access Control Rules across these 3 policies.

- 4 rules are about Sensitive Data
- 4 rules are about Internet Access
- 2 rules are about Internal Application Access

Regenerate

Ask a question or request, or type "/" for suggestions

Privacy policy Terms of service

Assist



Firewall ポリシーの構成

Augment



トラブルシューティング

Automate



ライフサイクル管理の規定

Video:

<https://www.cisco.com/site/au/en/solutions/artificial-intelligence/ai-assistant/index.html>

cdFMC / FMC 7.6 以降でサポート

Agenda

- 1 現在求められるFirewallの姿
- 2 FTD魅力ある新機能&保守運用効率化
4選 紹介
 - 2.1. バージョンとモデル遷移 おさらい
 - 2.2. 魅力ある新機能 4選
 - 2.3. 保守運用 効率化 4選
- 3 まとめ と Q&A

FTD バージョン遷移

2015年以前

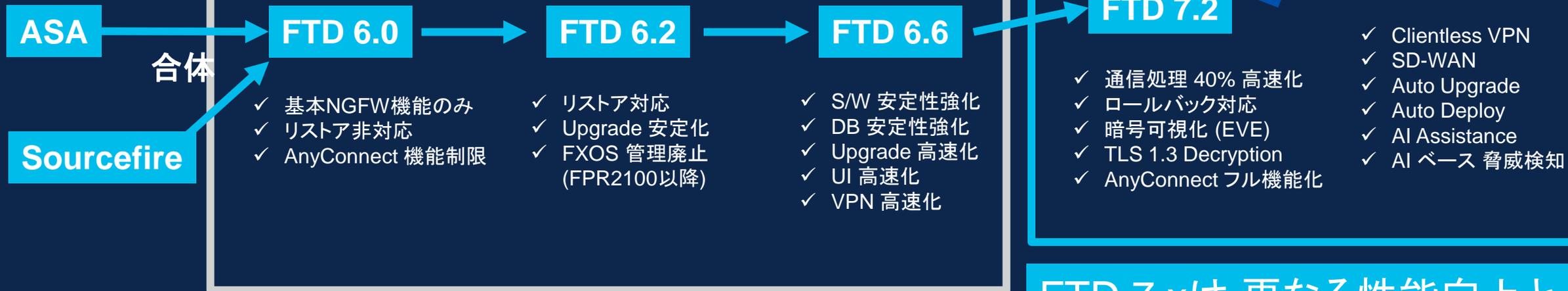
2017年

2019年

2021年

2023年

2025年～



- ✓ 基本NGFW機能のみ
- ✓ リストア非対応
- ✓ AnyConnect 機能制限

- ✓ リストア対応
- ✓ Upgrade 安定化
- ✓ FXOS 管理廃止 (FPR2100以降)

- ✓ S/W 安定性強化
- ✓ DB 安定性強化
- ✓ Upgrade 高速化
- ✓ UI 高速化
- ✓ VPN 高速化

- ✓ 通信処理 40% 高速化
- ✓ ロールバック対応
- ✓ 暗号可視化 (EVE)
- ✓ TLS 1.3 Decryption
- ✓ AnyConnect フル機能化

- ✓ Clientless VPN
- ✓ SD-WAN
- ✓ Auto Upgrade
- ✓ Auto Deploy
- ✓ AI Assistance
- ✓ AI ベース 脅威検知

FTD 6.xは、OS統合に伴う、既存機能の改修や安定化に注力

FTD 7.xは 更なる性能向上と魅力ある新機能リリースへ

モデル遷移

スループットは FTDで FW+AVC+IPS利用時 (1024bytes)

2015年以前

2017年

2019年

2021年

2023年

2025年～



ASA5500-X



Firepower 1010
880 Mbps



Firepower 1100
2.3 Gbps - 4.9 Gbps



Firepower 2100
2.6 Gbps - 10.4 Gbps



Firepower 4100
15.5 - 53 Gbps



Secure Firewall 1200C
3~6 Gbps



Secure Firewall 3100
17 Gbps - 45 Gbps



Secure Firewall 4200
65 Gbps - 140 Gbps

同価格帯で
数倍の性能向上！

同価格帯で数倍の性能向上！

同価格帯で数倍の性能向上！

NEW

NEW

NEW

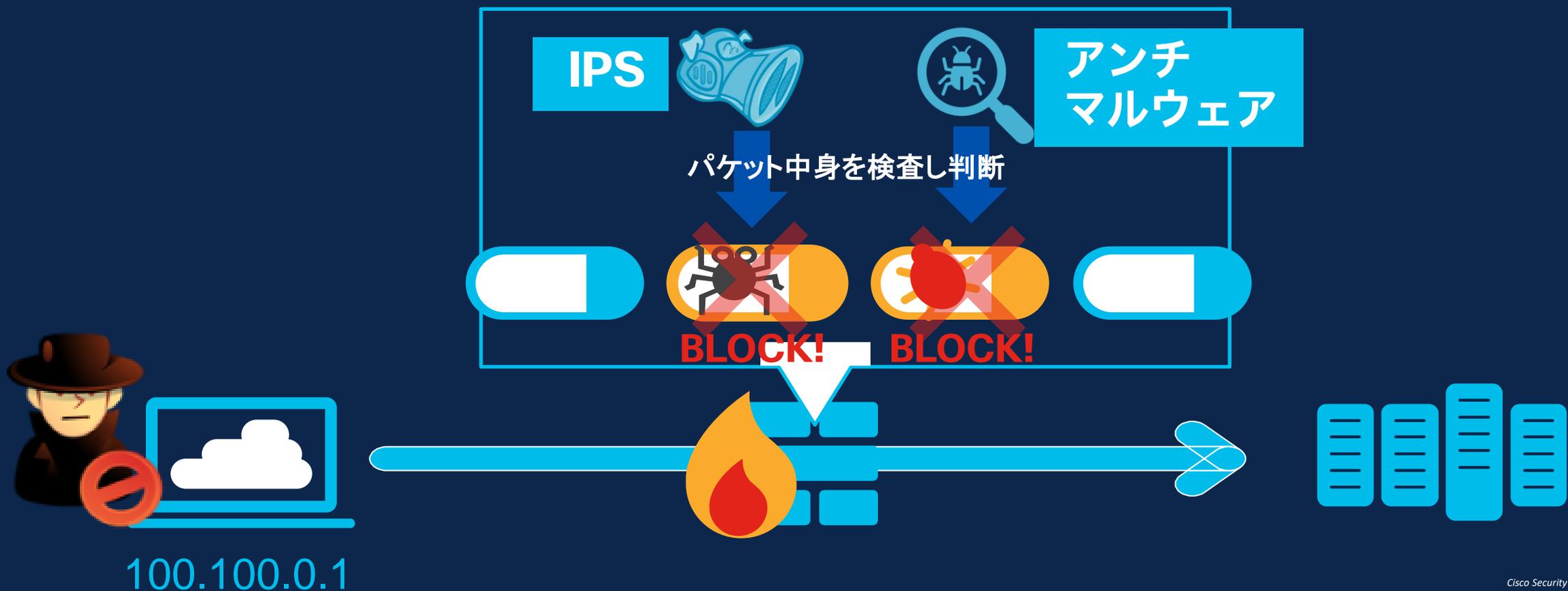
新規導入時は *Secure Firewall* モデルの利用を！

Agenda

- 1 現在求められるFirewallの姿
- 2 FTD機能改善と魅力ある新機能 紹介
 - 2.1. バージョンとモデル遷移 おさらい
 - 2.2. 魅力ある新機能 4選**
 - 2.3. 保守運用 効率化 4選
- 3 まとめ と Q&A

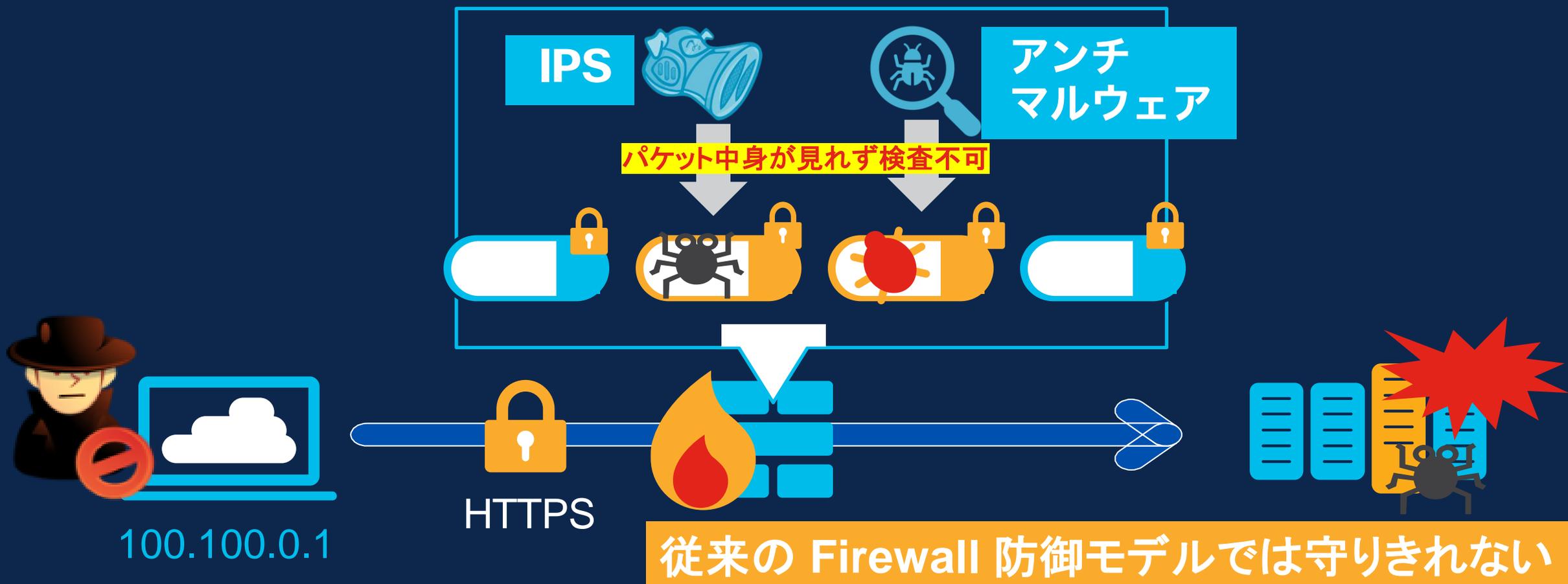
従来の Firewall 防御モデル

- 通信内に潜んだ不正コードやマルウェアをIPSやアンチマルウェアで検知・防御
- インターネット側のIPやDomain・URLの制御は困難



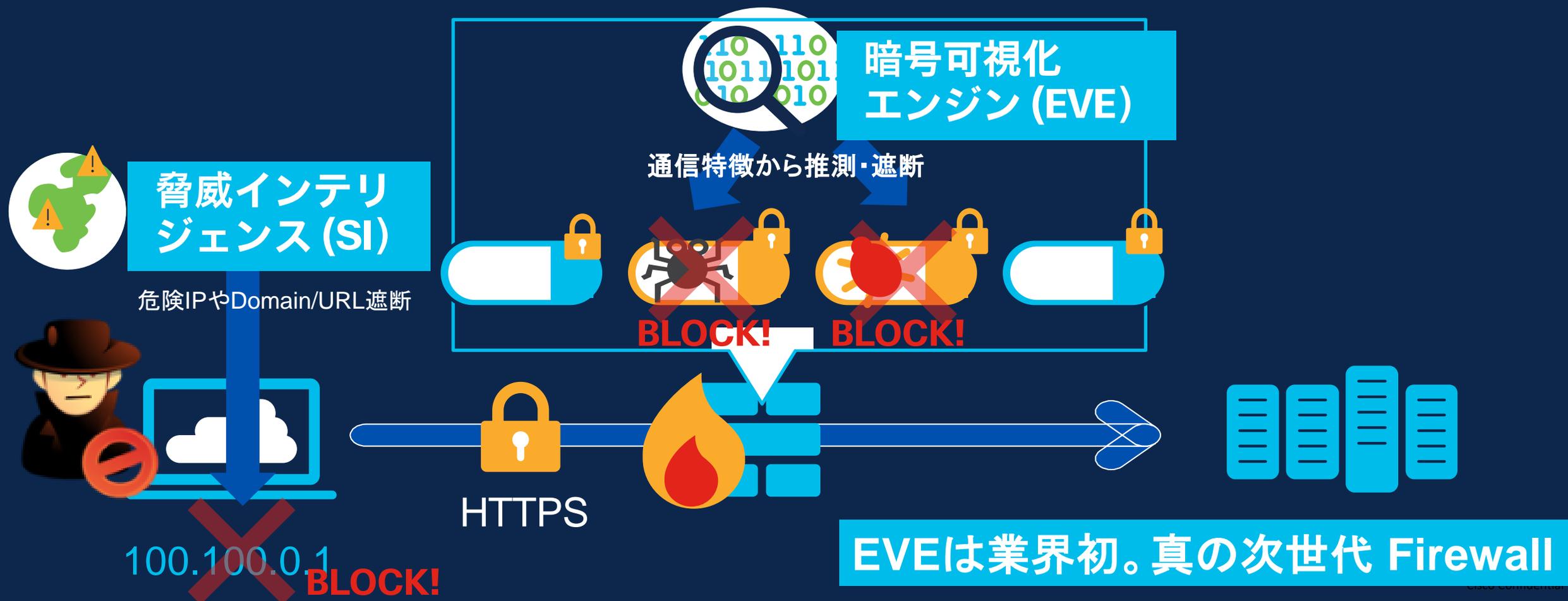
現在 インターネット通信の **約9割** が 暗号化通信

- 優れた検査エンジンでも、暗号化されたフローの前では効果が大きく減少
- 不正通信や情報流出の 5割は 暗号化通信



Cisco Secure Firewall (FTD) の新防御モデル

- ・ 暗号化された”まま”で「不正通信」の高速検査・遮断 (EVE)
- ・ インターネット上の 危険な IP や Domain・URL の高速検査・遮断 (SI)



魅力ある新機能 4選

業界初



暗号可視化
エンジン **EVE**

HTTPSやQUICを復号せず分析や脅威遮断



Opex削減

運用負荷 半減！？
AIアシスタント

長期未使用ACLや重複ACLの削除や、設定・運用支援など

AI & ML



ゼロデイ攻撃から保護
SnortML

シグネチャに頼らず、ゼロデイ攻撃から保護



業界標準

リモートアクセスVPN
1. AnyConnect
2. Clientless

より安全で快適な在宅勤務

魅力ある新機能 4選

業界初

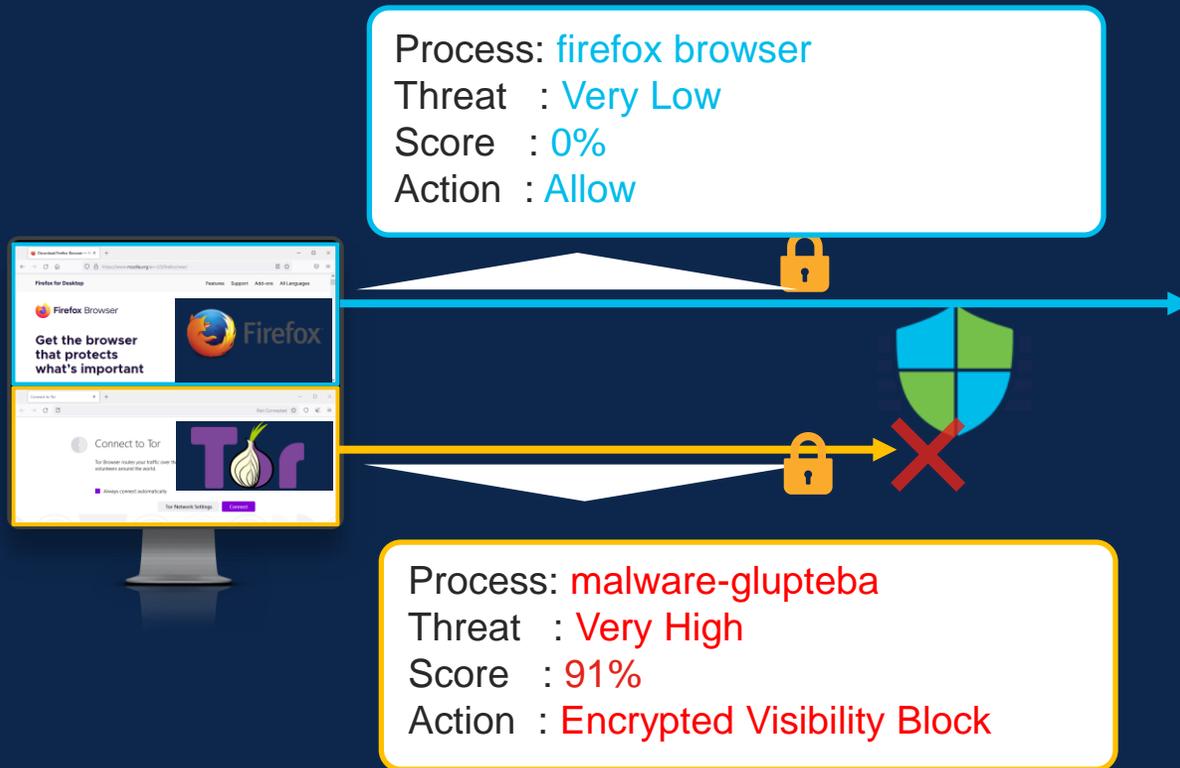
暗号可視化 エンジン EVE

HTTPSやQUICを復号せず分析や脅威遮断

✓ 暗号化通信を復号せず高速に検出・遮断

- TLS Fingerprint や ML など組み合わせた新技術
FTD 7.2以降でアプリ、7.4以降で脅威遮断に対応
- 従来の復号化技術 (TLS Decryption) と比べ、
低負荷・低遅延、かつ 通信影響発生リスク低

✓ 新暗号化通信 QUIC や HTTP/3にも対応



Firewall Management Center
Analysis / Unified Events

Showing all 27 events (1)

Time	Event Type	Action	Reason	Source IP	Destination IP
2024-02-17 12:25:26	Connection	Block	Encrypted Visibility Block	192.168.0.24	95.214.53.216
2024-02-17 12:25:25	Connection	Block	Encrypted Visibility Block	192.168.0.24	188.165.136.205
2024-02-17 12:25:24	Connection	Block	Encrypted Visibility Block	192.168.0.24	167.71.86.85
2024-02-17 12:25:19	Connection	Block	Encrypted Visibility Block	192.168.0.24	152.53.17.183

宣伝) SE Labs で最優秀ファイアウォールに選出

2023年と2024年 連続受賞!

この記事は、Cisco Security Business Group の Vice President & Chief Marketing Officer である Neville Letzerich によるブログ「SE Labs 2023 Annual Security Report Names Cisco as Best Next Generation Firewall」(2023/2/9) の抄訳です。



業界“初”の暗号可視化エンジン (EVE)

Cisco Secure Firewall の主な機能

SE Labs の年次レポート 2023 で、シスコが次世代ファイアウォール部門最優秀賞に選出されました。ごついて皆様にご報告できることを大変光栄に思っています。今回、業界で高い評価を得ることができたのは、ハイブリッド環境とマルチクラウド環境においてネットワーク、ワークロード、アプリケーションのセキュリティを調和させるというシスコの継続的な取り組みを認めていただけたからだと思います。Cisco Secure Firewall チームを大変誇りに思うと同時に、シスコを変わず信頼していただき、シスコの製品とソリューションを中心にネットワークセキュリティを着々と進化させていらっしゃる素晴らしいお客様に感謝を申し上げます。

SE Labs はサイバーセキュリティのテストと評価を実施している機関であり、さまざまなサイバーセキュリティ製品とソリューションについて、公平かつ独立したアセスメントを提供しています。SE Labs の年次レポート 2023 には次のような記述があります。

「Annual Security Awards は、当機関のテストで良好な結果を出しただけではなく、実際の顧客の実環境で高い成果を上げたセキュリティベンダーを表彰するものです。当機関のセキュリティ賞は、ラボ環境での優れた成果と実際の成功の両方を評価する、業界で唯一の賞です」

- 脅威に特化した Cisco Secure Firewall のアーキテクチャは、ネットワークトラフィックに対する優れた可視性と制御を実現します。多くのセキュリティ担当者は現在、暗号化されたトラフィックの可視化が難しいという悩みを抱えています。これが、シスコが独自の Encrypted Visibility Engine を開発した理由です。この可視化エンジンは、暗号化されたトラフィックを復号することなく、その中に潜む脅威を検出します。Cisco Secure Firewall の詳細な分析、可視化、レポート機能を利用すれば、ネットワークトラフィック、アプリケーション、アセットに関するインサイトをすばやく得られます。
- Cisco Secure Firewall の機能により、ネットワーク全体で統一されたセキュリティ態勢が実現します。これは、ワークロード、Web、電子メール、クラウドのセキュリティをシスコの SecureX XDR プラットフォームに緊密に統合することで可能になります。この統合により、脅威の調査と対応に要する時間が短縮され、SecOps チームの効率が向上します。
- Cisco Secure Firewall は、状況が変わりやすい環境に適応し、優れた拡張性を実現できるよう設計されており、総所有コストの削減が明確に設計で意図されています。Forrester Consulting に委託した第三者調査によると、Cisco Secure Firewall は一貫したポリシーの適用により、お客様のチームの作業時間短縮に貢献しており、3年間で最大 195% の投資利益率の達成に寄与しています。

常に進化を続けるサイバーセキュリティの世界では、最新かつ最も高度なテクノロジーを利用して脅威に先手を打つことが重要です。民間企業、政府機関、医療機関、サービスプロバイダー、あらゆるお客様に Cisco Secure Firewall は最高ランクのセキュリティを提供します。

<https://gblogs.cisco.com/jp/2023/08/se-labs-2023-annual-security-report-names-cisco-as-best-next-generation-firewall/>



魅力ある新機能 4選

AI & ML



ゼロデイ攻撃から保護

SnortML

シグネチャに頼らず、ゼロデイ攻撃から保護

✓ シグネチャに頼らないゼロデイ攻撃ブロック

- Cisco Talos が10年以上 開発・利用のML技術を活用
- 未知の SQL / Code / Command Injection をブロック
- 検知エンジンも日々学習し強化される

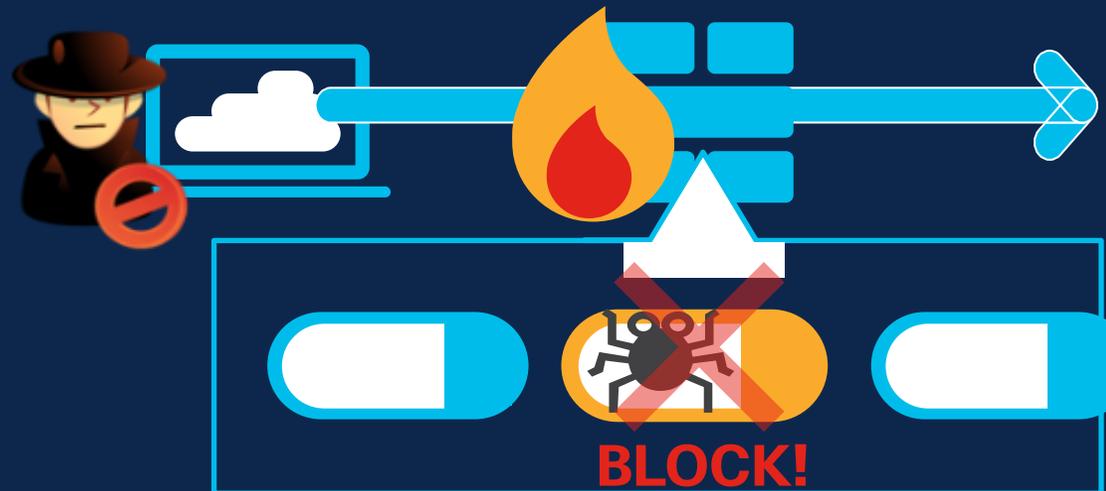
検知対象は
今後増加予定

✓ FTD 7.6 から対応



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

ゼロデイ攻撃



▼ Event Information

Message	(snort_ml) potential threat found in HTTP parameters via Neural Network Based
Time	2024-05-06 13:28:55
Classification	Unknown Traffic
Priority	low
Ingress Security Zone	BPInline
Egress Security Zone	BPInline
Device	10.7.117.156
Ingress Interface	10.20.0.1
Egress Interface	10.30.0.1
Source IP	10.20.34.251
Source Port / ICMP Type	5793 / tcp
Destination IP	10.30.10.157
Destination Port / ICMP Code	80 (http) / tcp
HTTP Hostname	10.30.10.157
HTTP URI	/joomla/index.php?option=com_saxumastro&view=savedreading&publicid=1'+

SnortMLで不正コード検知

魅力ある新機能 4選



Opex削減

運用負荷 半減！？
AIアシスタント

未使用や重複ACLの削除や、設定・運用支援など

✓ “AI”が設定や運用を”日本語”で強力支援

例1: ACLの重複や未使用ルール確認と無効化

例2: 特定設定を表形式で出力。パラメ簡単作成

例3: 設定やアップデート方法をガイド

例4: トラブル原因の切り分け支援

例5: 対話式での設定

✓ FTD 7.6 から対応

ACLの重複や未使用ルール確認と無効化

Policy Analysis and Optimization

Anomalies found from the initial scan: Out of 1234 rules, there are 323 duplicate rules found. These include 153 fully shadowed rules and 170 fully redundant rules.

Total rules 1234

- Fully Shadowed Rules (153)
- Fully Redundant Rules (170)

View Details ↗

We recommend you take one of the following actions on the duplicate rules:

Disable all Delete all

アップグレード方法ガイド

You
Firewallアップグレードを教えてください

AI Assistant
Cisco Secure Firewallのアップグレードには以下の手順が必要です：

ステップ1: Cisco Secure Firewall Management Center (FMC) にログインし、**Devices > Device Management**に移動して、**HA pair**のチェックボックスをクリックします。 **Select Action**をクリックし、Firepower Softwareをアップグレードを選択します。

ステップ2: アップグレードしたいバージョンを選択するために、**Select a version**をクリックします。

対話式でのACL設定

You
Webex Teamsのアプリケーションの通信をブロックしてください。Zoneは Guest から Public をお願いします。ログは残してください

AI Assistant

1 Rule Name

2 Section

3 Policy Name

Please provide Rule Name

参考) AI アシスタントでパラメータシート簡単作成

「Edge ACP」のアクセスコントロールポリシーの設定を、表で出力してください。その際に、以下の列を含んでください。アクセスリストの設定順番で並び替えてください。

- Name
- Action
- Source Zones and Networks and Ports
- Destination Zones and Networks and Ports

AI Assistant

Here are the details of the access control policies for Edge ACP. The policies are listed in the order they are set. Each policy has a name and an action associated with it. The policies also specify the source and destination networks, ports, and zones.

Showing 25 of 79 entries.

[Hide details](#)

	Policy Name	Action	Source Networks	Destination Networks	Source Ports	Destination Ports	Source Zones	Destination Zones
1	Research Access	ALLOW	None	research-server	None	tcp_32400 (TCP)	None	Users
2	DNG Access	ALLOW	None	access	None	DNS_over_TCP (TCP), DNS_over_UDP (UDP), HTTPS (TCP), HTTP (TCP)	Guest, Public, Users	Server
3	LOH Logs	ALLOW	publicserver.com	logs	None	tcp_10005 (TCP)	Public	Server

生成後は
エクセルやワードに
貼り付けるだけ！

Ask the AI Assistant a question



[View User Guide](#) to learn more.

魅力ある新機能 4選

業界標準

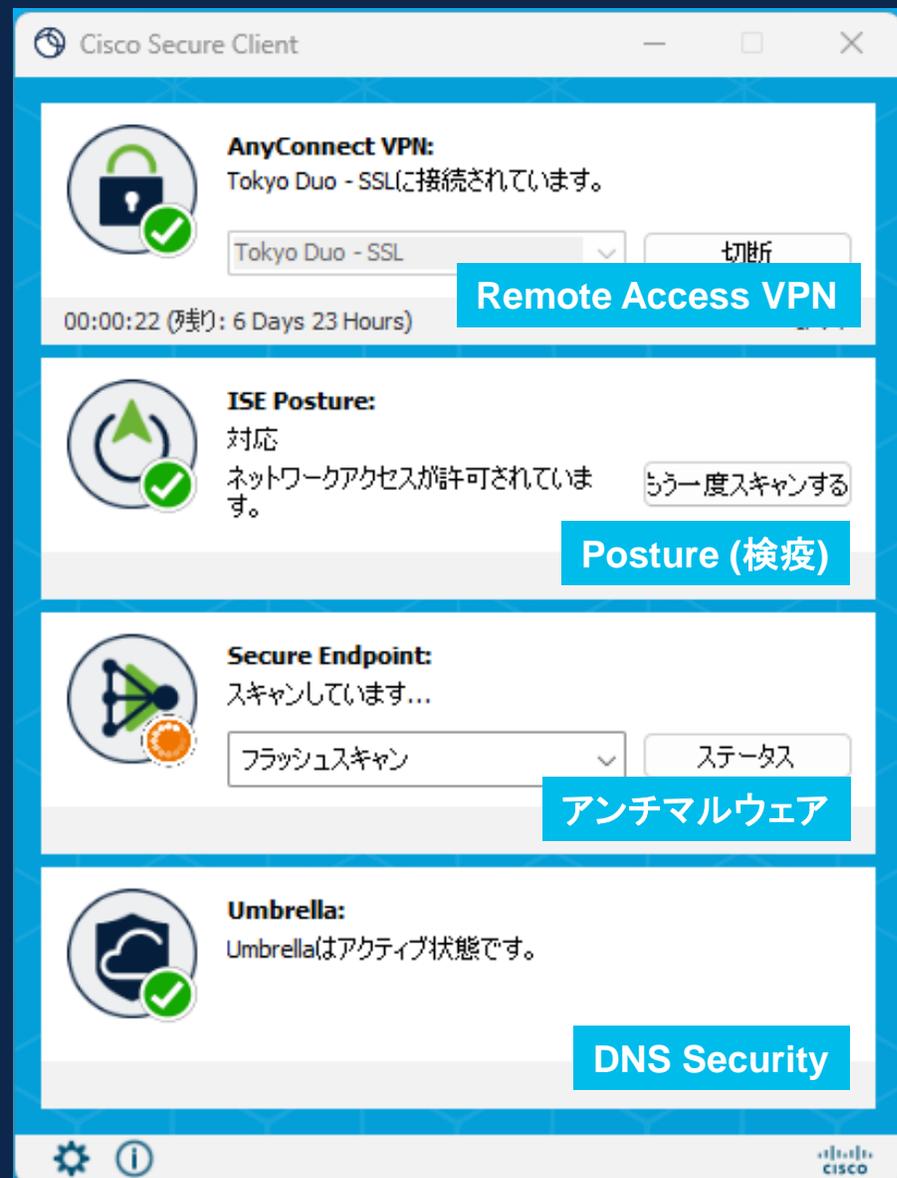


リモートアクセスVPN

1. AnyConnect
2. Clientless

より安全で快適な在宅勤務

- ✓ 利用実績 No.1「AnyConnect VPN」
 - ビジネスカテゴリ「VPN」App で 人気 1位*
 - FTD と ASA で、機能大差なし
 - 任意モジュールを追加可
Posture、アンチマルウェア、DNS Security、NetFlow
- ✓ FTD 7.4 から クライアントレス ZTNA 対応
 - Zero Trust Network Access。IPSやマルウェア検査と併用可



魅力ある新機能 4選



業界初

暗号可視化 エンジン **EVE**

HTTPSやQUICを復号せず分析や脅威遮断



Opex削減

運用負荷 半減！？ **AIアシスタント**

長期未使用ACLや重複ACLの削除や、設定・運用支援など

AI & ML



ゼロデイ攻撃から保護 **SnortML**

シグネチャに頼らず、ゼロデイ攻撃から保護



業界標準

リモートアクセスVPN 1. AnyConnect 2. Clientless

より安全で快適な在宅勤務

Agenda

- 1 現在求められるFirewallの姿
- 2 FTD魅力ある新機能&保守運用効率化
4選 紹介
 - 2.1. バージョンとモデル遷移 おさらい
 - 2.2. 魅力ある新機能 4選
 - 2.3. 保守運用 効率化 4選**
- 3 まとめ と Q&A

保守運用 効率化 4選

保守効率化



カンタンRMA
2時間 以内

FPR 1000/2100/3100/4200 でメンテナンスリリース利用時

Opex削減



リスクレポートで
ラクラク定期報告

脅威やマルウェアの検知状況サマリをレポート出力

Opex削減



カンタンIPS
自動で最適化

セキュリティを保ちつつ、誤検知や運用負荷を軽減



任意イベントを
管理者 通知

複数条件にマッチするイベントや 障害を管理者通知

保守運用 効率化 4選

保守効率化



カンタンRMA 2時間 以内

FPR 1000/2100/3100/4200 でメンテナンスリリース利用時

速習 Cisco **FPR1000/2100 SF3100/4200**

Reimage

RMAやダウングレード、FTDファイル破損時の復旧に有効です
Useful to repair FTD system in case of RMA, downgrade or system recovery

<https://youtu.be/wUxp7i3Tuh8?si=a627rOsyXwVS7Lc7>

速習 Cisco **FPR4100 専用**

FPR4100-FTD Reimage

RMAやダウングレード、ファイルシステム破損時の復旧に有効です
Useful for RMA, downgrade and repair FXOS/FTD file system

<https://www.youtube.com/watch?v=i0cgn2PT-k4>

4100は手順が異なり RMA 4時間～目安

✓ FTD 保守交換が 最短 4ステップで可能

1. 良品リイメージ
2. FTD 設定リストア
3. FTD HA 有効化 (*冗長構成で利用時のみ)
4. FMCから最新設定を適用

Note: FTDバージョンはメンテナンスリリース*の利用を
*バージョン桁数が3桁目までの、パッチ適用不要バージョン
例:7.2.5や7.2.8、7.0.6 など

速習 Cisco FMC / FTD Quick Study **FTD共通**

Restore

予め取得していたバックアップファイルを利用し設定復元します
Restore setting by using previously obtained backup file

<https://www.youtube.com/watch?v=NR-x9vc9cwM&t=0s>

保守運用 効率化 4選



カンタンIPS 自動で最適化

セキュリティを保ちつつ、誤検知や運用負荷を軽減

Opex削減

- ✓ 保護レベルは3つのベースポリシーから選択
Cisco がポリシー内ルールを定期更新
 - L1 Connectivity: 速度優先 (CVSS10)
 - L2 Balanced : 中間 (CVSS 9以上)
 - L3 Security : セキュリティ優先 (CVSS 8以上)
- ✓ 「ルール推奨」機能でルール最適化
 - 通信分析し不要ルールを削除し、誤検知や負荷の軽減に

ルール最適化“前” L2 Balanced の場合

Block	Alert	Total	Setting
8,845	469	9,314	Starting policy*



ルール
推奨機能

Secure Firewall Rule Recommendations

Security Level (Click to select)

Accept Recommendation to Disable Rules

No Impact - No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks

Cancel Generate Generate and Apply



ルール最適化“後”

Block	Alert	Total	Setting
5,783	233	6,016	Higher Efficiency

ルール 3割 圧縮

保守運用 効率化 4選

Opex削減



リスクレポートで ラクラク定期報告

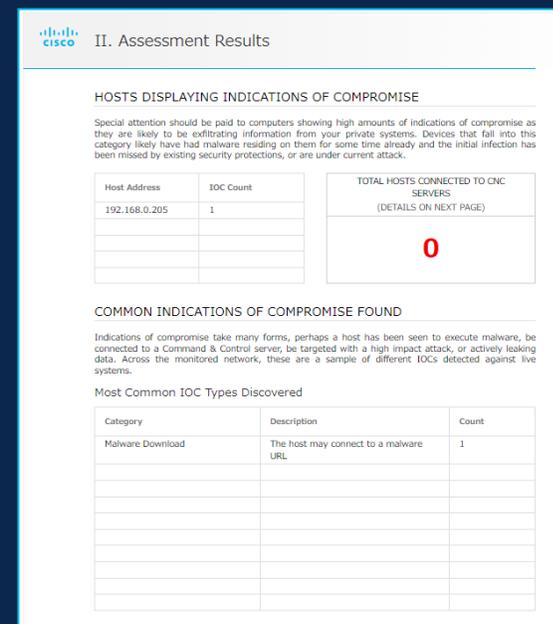
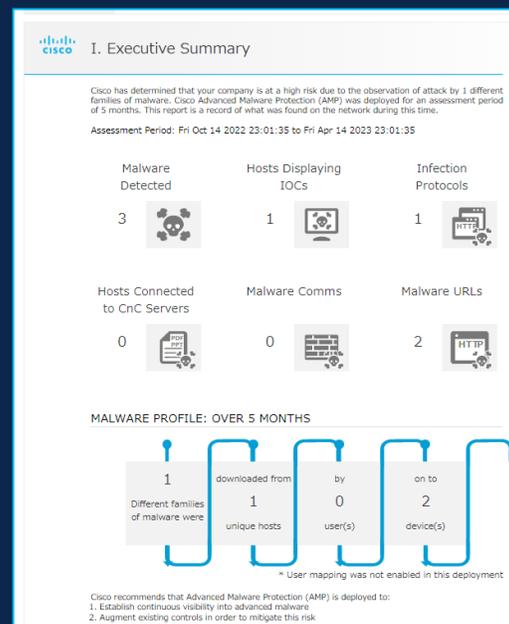
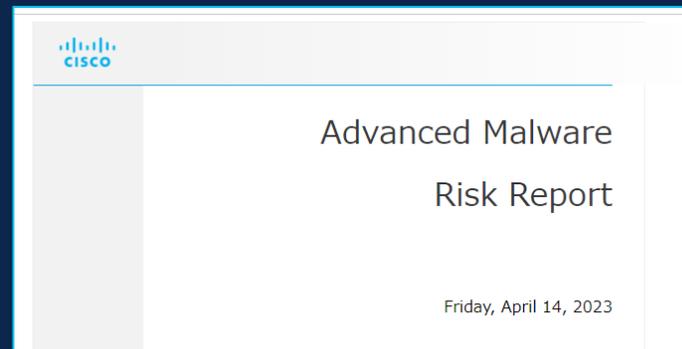
脅威やマルウェアの検知状況サマリーをレポート出力

✓ 数クリックでサマリーレポート生成

- 攻撃リスク (IPSによる脅威検知状況)
- ネットワークリスク (リスクの高いアプリケーション)
- マルウェアリスク (ランサムウェアや未知ファイル)

✓ レポートは PDF もしくは HTML

- HTMLの編集も可能



保守運用 効率化 4選

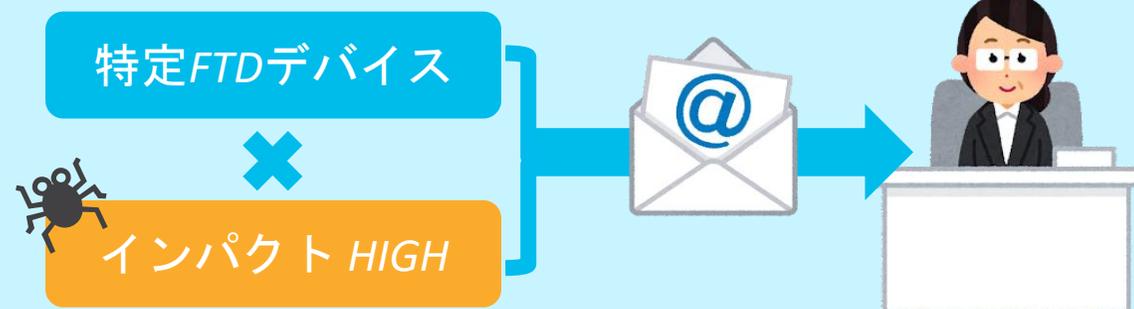


任意イベントを 管理者 通知

複数条件にマッチするイベントや 障害を管理者通知

- ✓ 「**相関ポリシー**」で複数条件合致時に通知
 - IPS、Malware、Connection、VPNイベントなど
 - 検知デバイス、端末IPやユーザ名、脅威インパクトなど
- ✓ 「**ヘルスポリシー**」で機器状態や障害通知
 - CPU、メモリ、Disk、VPN、Hardware障害など
- ✓ 通知方式はメールや Syslog・SNMP対応

運用例 ①「脅威の自動通知」



<https://community.cisco.com/t5/-/-/ta-p/3165340>

運用例 ②「機器状態や障害通知」



<https://community.cisco.com/t5/-/-/ta-p/3292677>

保守運用 効率化 4選

保守効率化



カンタンRMA
2時間 以内

FPR 1000/2100/3100/4200 でメンテナンスリリース利用時

Opex削減



リスクレポートで
ラクラク定期報告

脅威やマルウェアの検知状況サマリをレポート出力

Opex削減



カンタンIPS
自動で最適化

セキュリティを保ちつつ、誤検知や運用負荷を軽減



任意イベントを
管理者 通知

複数条件にマッチするイベントや 障害を管理者通知

Agenda

- 1 現在求められるFirewallの姿
- 2 FTD魅力ある新機能&保守運用効率化
4選 紹介
 - 2.1. バージョンとモデル遷移 おさらい
 - 2.2. 魅力ある新機能 4選
 - 2.3. 保守運用 効率化 4選
- 3 まとめ と Q&A

まとめ

- 新 *Cisco Secure Firewall 1200C* と *3100* シリーズはコスパ最強
- 従来型 *Firewall* では、企業セキュリティを守りきれない
 - インターネット通信の約9割が暗号化通信であり、*IPS*やアンチマルウェア検査が困難
 - 復号技術 (*TLS Decryption*) は遅延や通信不安定化リスクが高く、実用が困難
- *Cisco Secure Firewall (FTD)* は真の次世代 *Firewall*
 - 暗号可視化エンジン・・・業界初！暗号化された“まま”で「不正通信」の高速検査・遮断
 - *SnortML*・・・AI/MLを活用した、日々進化するゼロデイ攻撃検知エンジン
 - *AIアシスタント*・・・AIによるACL最適化や設定・運用支援
 - リモートアクセスVPN・・・実績豊富な「*AnyConnect VPN*」や「クライアントレス *ZTNA*」対応
- シンプルなRMA、カンタン *IPS* 自動最適化、リスクレポート、柔軟な通知機能など、運用負荷軽減に役立つ機能盛りだくさん
- お客様やパートナー様に、長く愛される *Firewall* へと進化を続けます

まとめサイト「FTD How To」

2024年2月 公開！
毎月更新！

Cisco Secure Firewall (FTD) – How To

当サイト「Cisco FTD How To」は、Secure Firewall Management Center (FMC) 管理の Firewall Threat Defense (FTD) の、新着情報や、提案や設計、設定や検証、保守運用、トラブルシューティングに役立つ情報のまとめサイトです。毎月更新。

なお、🔒 はシスコ契約アカウント、🔑 はパートナー契約アカウントをお持ちの場合に、アクセス可能なコンテンツです。掲載や更新のご要望や、リンク切れや不備などございましたら、[アンケート](#) よりご連絡ください。

- 新着ニュース・イベント
- 注意喚起
- 推奨ソフトウェアバージョン
- All-in-one 導入ガイド
- 提案・設計資料
- FMC 機能
- FTD デバイス 設定
- FTD 通信制御 機能
- FTD VPN 機能
- 保守・トラブルシューティング
- おすすめ ブログ
- よくある質問
- 関連情報

新着ニュース・イベント

新着ニュース

- FTD 最新版 7.4.1 がリリースされました！(リリースノート/新機能紹介)

イベント情報

- 7月10日(水)「バージョン 7.2.7+ オススメ機能とアップグレード ベストプラクティス」(LINK)
- 7月18日(木)「Firewall Roadshow」申し込みは [コチラ](#) オススメ！
 - 10:00～「最先端のFirewall新機能紹介 - あなたのセキュリティを次のレベルへ」
 - 10:45～「競合FW構築経験者が語る - Firewall Migration Tool を活用した移行方法」

FTD の提案や設計、導入・保守運用に必要な情報が揃った、オールインワンサイト！

Cisco SE や TAC・CSが 総力をあげて作成・監修

- ✓ 新着ニュースや イベント、推奨バージョン情報
- ✓ 注意喚起情報
- ✓ 提案・設計 資料
- ✓ 主要機能の設定やデモガイド
- ✓ 運用や保守ガイド
- ✓ おすすめブログ記事、など

<https://cs.co/ftd>

FTD Upgrade や RMA、
Migration 方法も記載アリ

ASA や 他社 Firewall から簡単マイグレーション



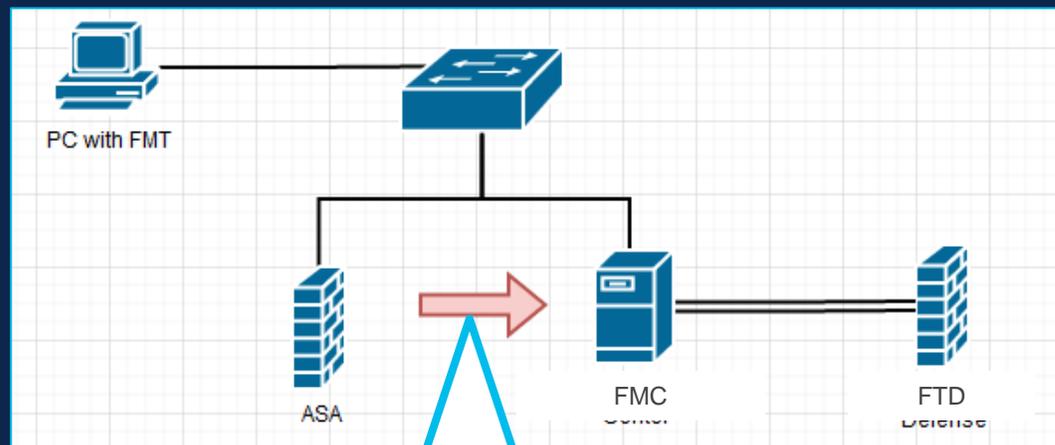
簡単マイグレーション Firewall Migration Tool (FMT)

ASA・Palo Alto・Fortinet・Checkpoint 対応

- ✓ ASAや他社Firewall 設定ファイルを利用し、FMC/FTDに簡単 設定展開

移行可能な設定:

1. ACL、NAT、Object/Object Group
2. Interface や VLAN、Channel
3. Static / Dynamic Routing
4. サイト間 VPN、Remote Access VPN



The screenshot shows the 'Firewall Migration Tool (Demo Mode)' interface. The main section is titled 'Extract Cisco ASA (8.4+) Information'. It contains two columns of options: 'Manual Upload' and 'Connect to ASA'. The 'Manual Upload' section lists instructions for file formats (.cfg or .txt), context types (Multi-context vs Single-context), and warnings against hand-coded configurations and files larger than 1MB. The 'Connect to ASA' section prompts for management IP address and admin credentials, with a field for 'ASA IP Address/Hostname' and a 'Connect' button. At the bottom, there are sections for 'Primary Context Selection' and 'Parsed Summary'.

設定ファイルをアップロード後、
ウィザードに沿って操作で移行完了

全体

Q & A

モヤモヤでも何でもお気軽に！





機能改善 4選 - 旧 Version 6.xとの比較



処理性能 平均
40% アップ

Snort 3 利用時



アップグレード
30% 高速化



ロールバック
対応



UI 改善
より見やすく
より探しやすい

機能改善 4選



処理性能 平均
40% アップ

Snort 3 利用時

✓ 次世代NGFWエンジン Snort 3

- FTD 7.x のデフォルト
- 処理性能や メモリ利用効率を改善

✓ IPS 検知性能も向上

- 次世代HTTPインスペクタ対応
- より膨大なIPSルール 並行処理可能に



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

Superior Performance

Firepower Threat Defense 7.0 Performance Improvements with Snort3

Model	NGFW Throughput	VPN Throughput
Firepower 1000 Series	Up to 40%	Up to 80%
Firepower 2000 Series	Up to 20%	Up to 25%
Firepower 4000 Series	Up to 30%	Up to 50%
Firepower 9000 Series	Up to 60%	Up to 40%
Firepower Virtual	Up to 10% for VMW/KVM & up to 100% for Azure	Up to 40%

Snort 2 vs. Snort 3

バージョン 7.0 より Snort 3 エンジンをサポート

	Snort 2	Snort 3
マルチスレッドアーキテクチャ		✓
複数の Snort プロセス稼働	✓	✓
ポート番号から独立したプロトコルのインスペクション		✓
IPS でのアクセラレータ/ハイパースキャンをサポート		✓
モジュール性 - TALOS からの情報を容易に取り込み		✓
スケーラブルなメモリ割り当て		✓
次世代 TALOS ルール - 正規表現 / ルール最適化 / バッファ		✓
新しい HTTP インスペクタ - HTTP/2 をサポート		✓
TALOS からのアップデートを小型化		✓

機能改善 4選



ロールバック 対応

- ✓ 設定や IPS ルール、VDB*の10世代前までのロールバック対応
 - 設定変更後の不慮の通信断発生時、素早い切り戻しが可能に
- ✓ アップグレードリバート
 - 失敗時に自動 or 手動で前バージョン切り戻し

Rollback

▲ Rollback is the last resort for disaster recovery. Use rollback only if a deployment has caused a data traffic out

Choose devices from Job Device List

Selected Job ▼
User:admin; Deployed on:Feb 18, 2023 11:59 PM

<input checked="" type="checkbox"/>	Device	Rollback Version	Preview
<input checked="" type="checkbox"/>	CoreFTD-FPR1010	Feb 18, 2023 1:16 PM ▼	
		Feb 18, 2023 1:16 PM <i>Scheduled_Deploy_Job_215</i>	Deployment after SRU/LS
		Feb 15, 2023 1:23 PM <i>Scheduled_Deploy_Job_214</i>	Deployment after SRU/LS
		Feb 10, 2023 1:23 PM <i>Scheduled_Deploy_Job_213</i>	Deployment after SRU/LS

機能改善 4選



アップグレード
30% 高速化

✓ アップグレード内部処理を最適化

- 互換性や健全性の事前チェック機能も追加
- 1台あたり 概ね 1時間で可能に

✓ ver 7.4+ オートアップグレード機能

- ワンクリックで簡単アップグレード

ファイル展開から、互換性・健全性確認、アップグレード、失敗時のログ収集やロールバックまで自動実行



Auto Upgrade 機能 (FTD 7.4-)

System Overview

Management Center: 7.4.1-172
Already running latest version.
Last upgrade performed: 7.2.5-208 → 7.4.1-172

Available Upgrade Packages

These are the downloadable upgrades that are currently configured.

Upgrade	Release Date	Version
7.4.1-172	2023-12-13	7.0.0
Cisco Secure Firewall Management Center		
Firepower 1000 series with FTD		
> 7.3.1-19	2023-03-09	7.0.0
> 7.3.0-69	2022-11-28	7.0.0
> 7.2.5-208	★ Suggested	
> 7.2.4-165		

ワンクリックで
アップグレード
ファイル取得

推奨verを
FMCから確認可

機能改善 4選



UI 改善
より見やすく
より探しやすい

✓ 全イベントを1画面で確認可能に

- Unified Event 機能。表示イベントは ON/OFF 可
IP/Portやアプリ/URL、脅威、マルウェア、EVE、SSL Type等

✓ デバイスのヘルス情報も1画面で

- プロセス、キャパシティ、CPU、メモリ、ディスク使用量など

Unified Event

Overview Analysis Policies Devices Objects Integration Deploy

Showing all 2,191 events (2,191 2)

Time	Event Type	Action	Reason	Source IP	Destination IP
2022-06-14 16:46:18	Connection	Allow			64.104.14.229
2022-06-14 16:46:16	Connection	Allow			173.37.151.30
2022-06-14 16:46:15	Connection	Allow			173.37.151.30
2022-06-14 16:46:08	Security Intelligence	Block	IP Block	192.168.0.201	102.130.113.9
2022-06-14 16:46:00	Connection	Allow			208.67.222.222
2022-06-14 16:45:52	Security Intelligence	Block	IP Block	192.168.0.201	101.3.121.242
2022-06-14 16:45:47	Connection	Allow			64.104.14.229
2022-06-14 16:45:41	Connection	Allow			192.111.4.109
2022-06-14 16:45:39	Connection	Allow		192.168.0.201	23.67.167.18

