Cisco
Customer Experience

Ask the Experts

機能概要：
アクセスコントロールとマルウェア ポリシーとファイルポリシー

2024 年 4 月 10 日

Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

本日の学習内容

アクセス コントロール ポリシー (ACP) のコンポーネントを理解する

マルウェアとファイルポリシーを理解する

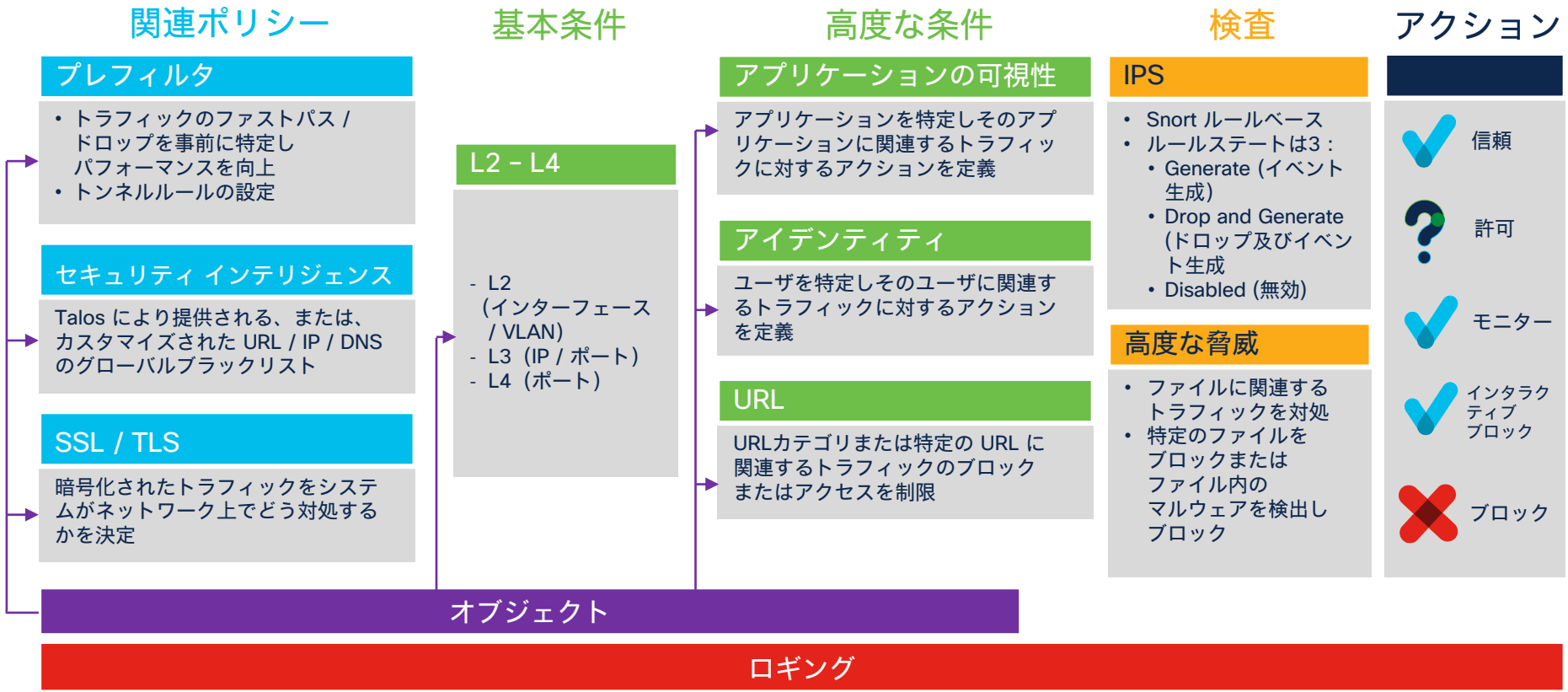
ポリシー設定のベストプラクティスについて学習する

アジェンダ

1. アクセス コントロール ポリシー
2. マルウェアとファイルポリシー
3. ベストプラクティスの概要

アクセス
コンロール
ポリシー

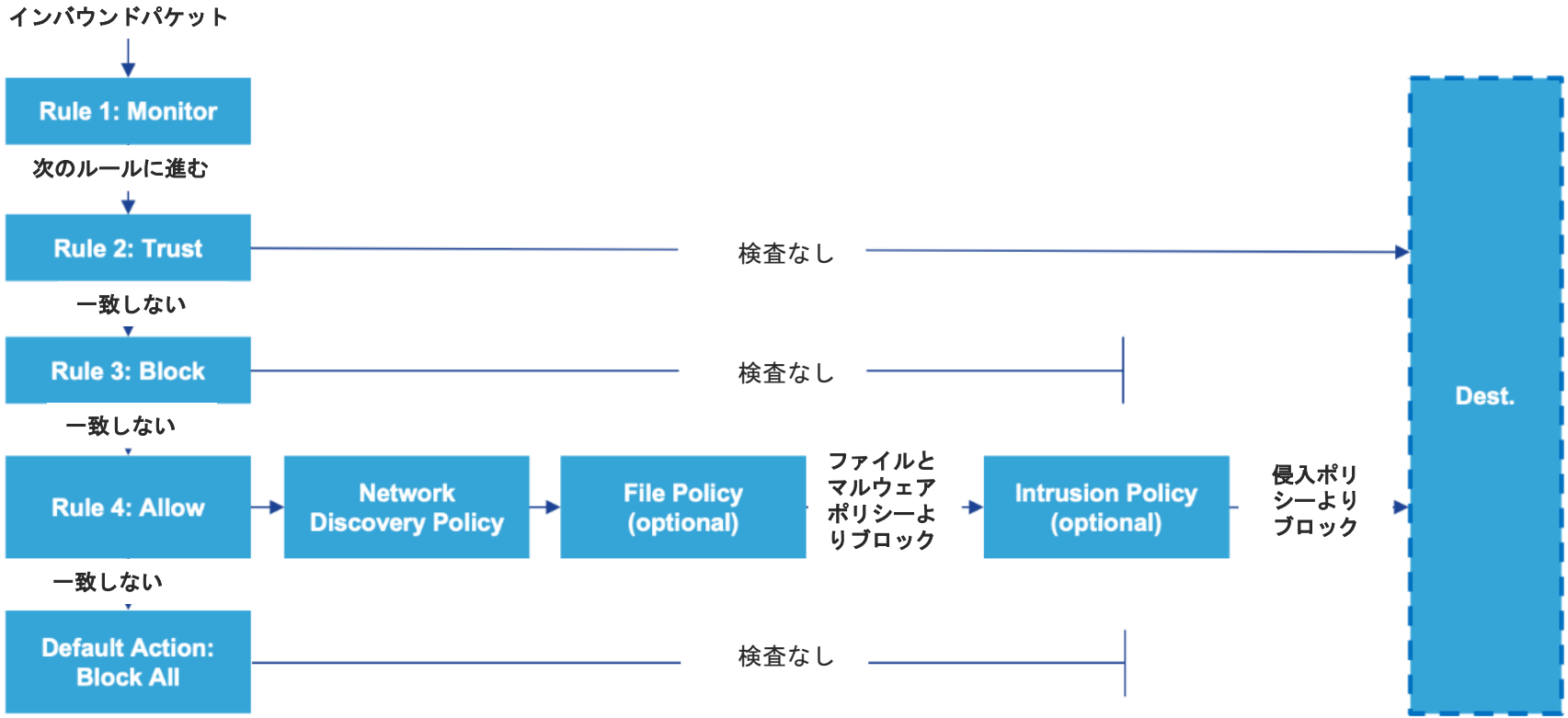
アクセス コントロールポリシーのコンポーネント



アクセスコントロール ポリシーのアクション

アクションの詳細		結果
信頼（Trust）	トラフィックを即座にパス	パス
許可（Allow）	IPS /ファイルルールの検査	ドロップまたはパス
モニター（Monitor）	トラフィックのログのみ	パス
インタラクティブブロック (Interactive Block)	ブロックするが、ユーザバイパスを許可	パス
ブロック（Block）	トラフィックのドロップ	ドロップ

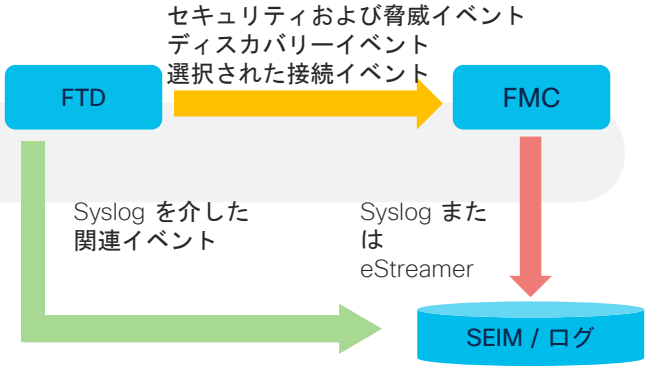
アクセス コントロール ルールの処理



ログ

デフォルトでログに記録されるイベント

- セキュリティ インテリジェンスイベント
- ファイル イベント
- マルウェアイベント
- 侵入イベント
- インテリジェント アプリケーション バイパスイベント



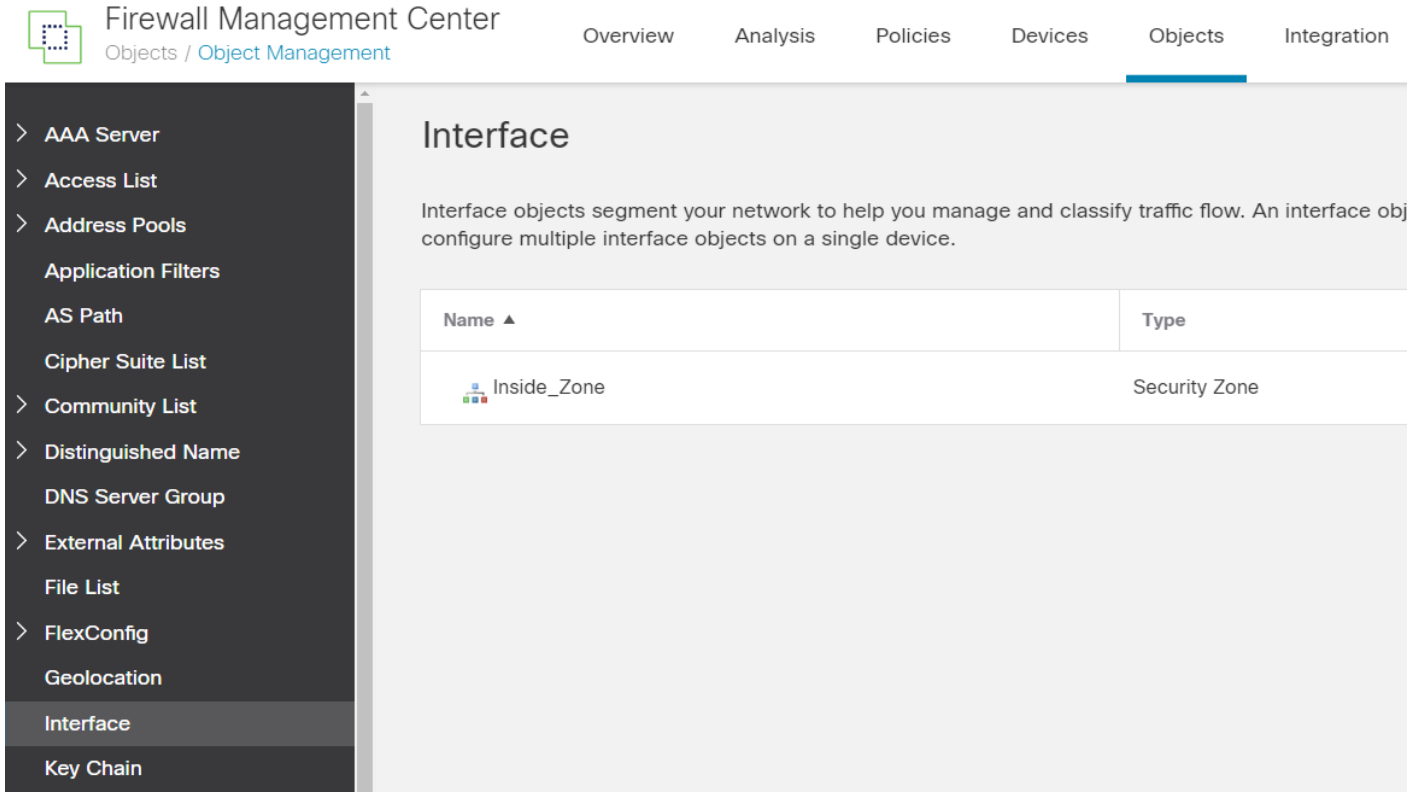
ログの内容

- 信頼アクションのないアクセス制御ごとの接続ログ
- 重要なログのみ

外部ソースへのロギング

- 長期間保持するために外部または SEIM へのログ共有が可能
- eStreamer またはアラート応答を介したロギング（Syslog または SNMP トラップ）

オブジェクトの活用



オブジェクトタイプの概要

Firewall ポリシー

異なるポリシータイプの更新頻度は？

頻繁	時々	ほとんどない
• アクセス コントロールポリシー • 侵入ポリシー	• マルウェアとファイルポリシー • アイデンティティ ポリシー • プレフィルタ ポリシー	• ネットワークディスカバリーポリシー • ネットワーク分析ポリシー • Correlation ポリシー • ヘルスポリシー • SSL ポリシー • DNSポリシー

デモ：

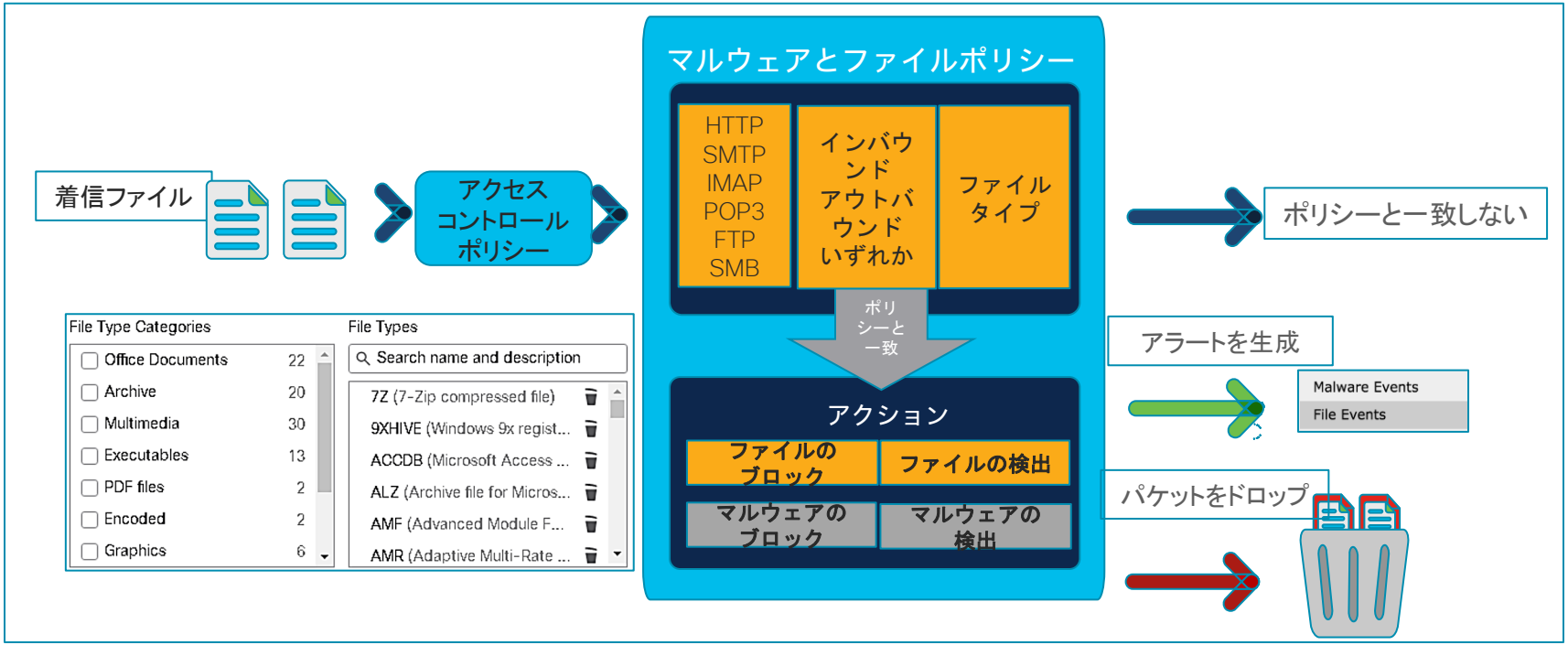
アクセス コントロール ポリシー

マルウェアとファイル ポリシー

ライセンス要件

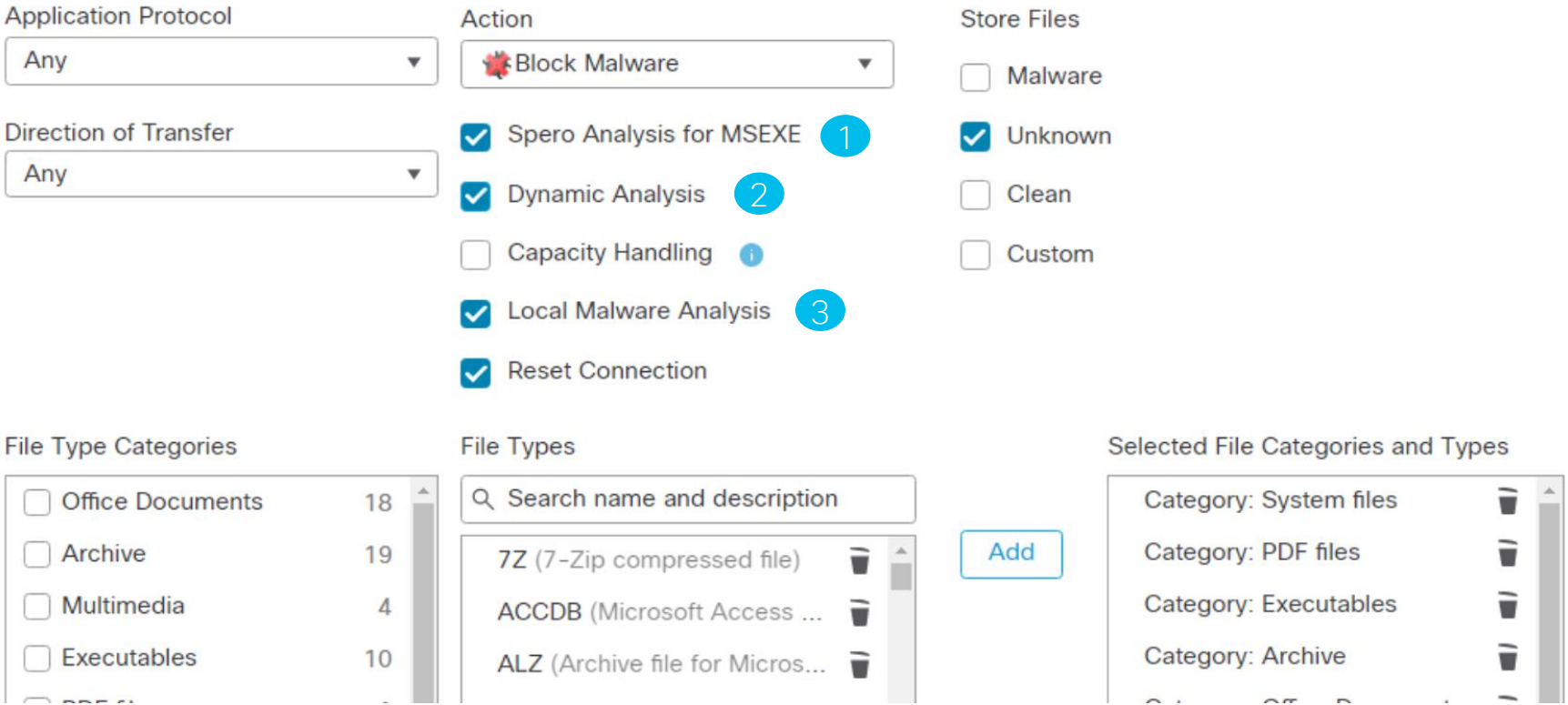
利用したい機能	必要なライセンス	必要なライセンス（7.3 以降）
特定のタイプのすべてのファイルをブロックまたは許可する（たとえば、すべての .exe ファイルをブロックする）	Threat	IPS
マルウェアが含まれている、またはマルウェアが含まれている可能性があるとの判断に基づいて、ファイルを選択的に許可またはブロックする	Threat, Malware	IPS, Malware Defense
ファイルの保存	Threat, Malware	IPS, Malware Defense

マルウェアとファイルポリシー



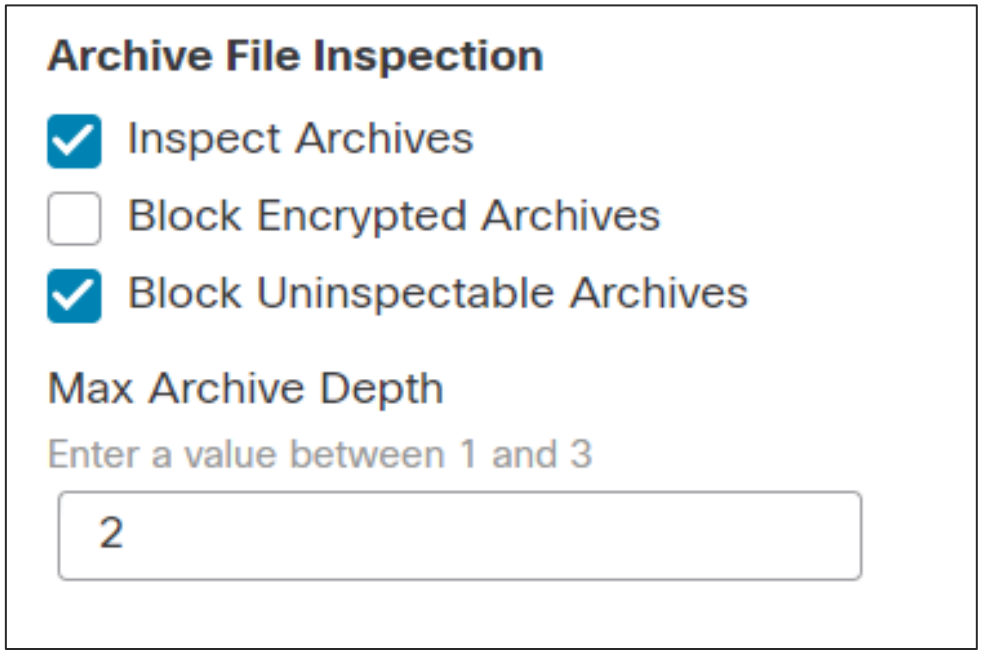
マルウェアとファイル ポリシー

Policy > Malware & File

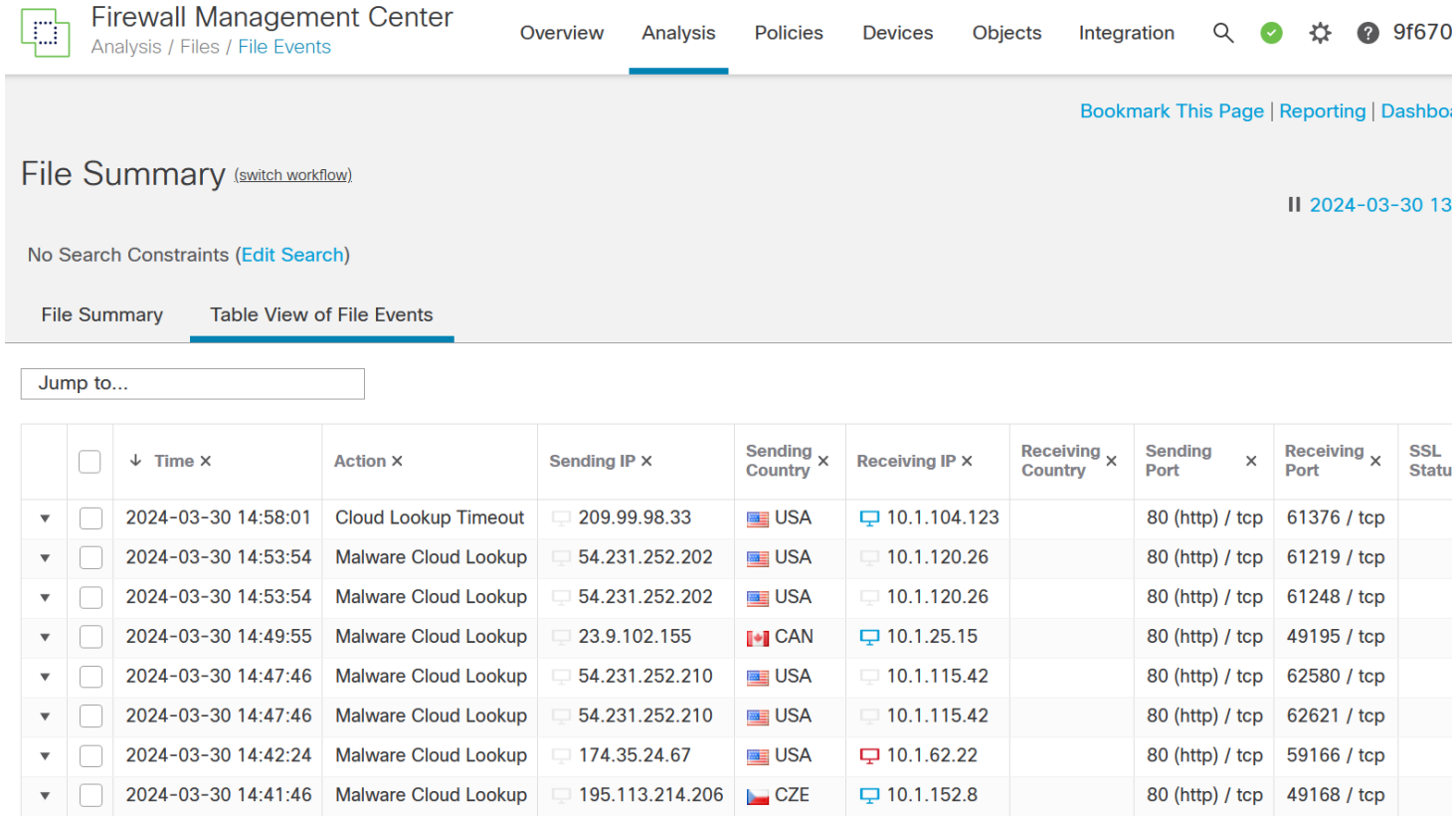


圧縮ファイルの検査

- デフォルト無効
- Policy > Malware & File > Advanced



ファイルイベント



Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	SSL Statu
2024-03-30 14:58:01	Cloud Lookup Timeout	209.99.98.33	USA	10.1.104.123		80 (http) / tcp	61376 / tcp	
2024-03-30 14:53:54	Malware Cloud Lookup	54.231.252.202	USA	10.1.120.26		80 (http) / tcp	61219 / tcp	
2024-03-30 14:53:54	Malware Cloud Lookup	54.231.252.202	USA	10.1.120.26		80 (http) / tcp	61248 / tcp	
2024-03-30 14:49:55	Malware Cloud Lookup	23.9.102.155	CAN	10.1.25.15		80 (http) / tcp	49195 / tcp	
2024-03-30 14:47:46	Malware Cloud Lookup	54.231.252.210	USA	10.1.115.42		80 (http) / tcp	62580 / tcp	
2024-03-30 14:47:46	Malware Cloud Lookup	54.231.252.210	USA	10.1.115.42		80 (http) / tcp	62621 / tcp	
2024-03-30 14:42:24	Malware Cloud Lookup	174.35.24.67	USA	10.1.62.22		80 (http) / tcp	59166 / tcp	
2024-03-30 14:41:46	Malware Cloud Lookup	195.113.214.206	CZE	10.1.152.8		80 (http) / tcp	49168 / tcp	

ネットワークファイルトラジェクトリー

Firewall Management Center
Analysis / Files / Network File Trajectory

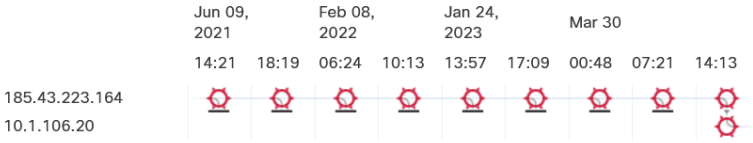
Overview | Analysis | Policies | Devices | Objects | Integration

Network File Trajectory for d2da2486...44b1f08e

File SHA256	d2da2486...44b1f08e
File Name	term.xbel
File Size (KB)	42.503
File Type	SWF
File Category	Multimedia
Current Disposition	Malware
Threat Score	Very High
Detection Name	SWF.Exploit.Kit.tht.VRT

First Seen	2021-06-09 14:21:33 on 185.43.223.164 jayda ball (dcloud.cisco.com\jball, LDAP)
Last Seen	2024-03-30 14:13:21 on 10.1.106.20 by
Event Count	9
Seen On	2 hosts
Seen On Breakdown	1 sender → 1 receiver

Trajectory



Events: Transfer, Block, Create, Move, Execute, Scan, Retrospective, Quarantine
Dispositions: Unknown, Malware, Clean, Custom, Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposit	Action	Protocol
2021-06-09 14:2...	Transfer	185.43.223.164	10.1.109.65	jayda ball (dcloud....	term.xbel	Mal...	Malware Block	HTTP
2021-06-09 18:1...	Transfer	185.43.223.164	10.1.101.127	grace murphy (dcl...	term.xbel	Mal...	Malware Block	HTTP

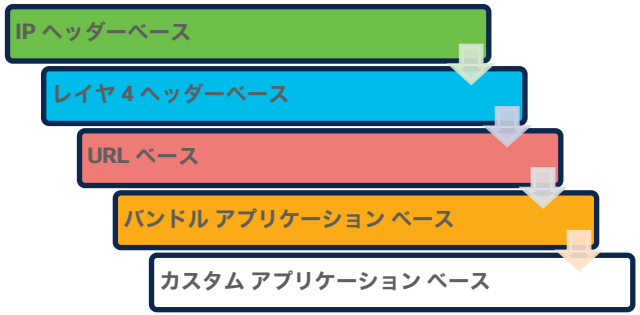
デモ：

ファイルとマルウェアポリシー

ベストプラクティス

アクセス コントロールポリシーの ベスト プラクティス

- 最適なルール 順序を使用する



- オブジェクトとオブジェクトグループを使用してルール数を制限
- バージョン 7.2 では、ポリシーをロックすることを推奨。アクセス コントロール ポリシー ロック機能により、管理者はポリシーをロックして、他の管理者が編集できないようにすることが可能

マルウェアとファイルポリシーのベストプラクティス

- [ファイルのブロック] および [マルウェアのブロック] アクションを利用する場合、 [接続をリセットする」 オプションも有効にする
- 大量のトラフィックをモニタしている場合、キャプチャしたファイルを全部保存することをしない
- マルウェア機能を有効にした場合、機器全体のパフォ−マンスに影響が発生するため、常時利用しない場合は 設定を無効化にする
  - 暗号通信のマルウェア検知は TLS Decryption 併用必要。両機能の利用時は 、十分なパフォーマンスを確保する必要がある
  - 必要な通信のみ暗号解読・マルウェア検知するよう設定し負荷を軽減する
  - アンチマルウェアを活用する場合、AVC/IPS/URLフィルタリングのみ利用時に比べ、ワンランク上のモデル利用が安定

覚えておくべき重要なポイント

01 ACP のコンポーネントとパケットフローを理解する

02 パフォーマンスを最適化するために、最初から不要なファイルタイプをブロックする

03 マルウェアとファイル保護機能を有効にするために必要なライセンス があることを確認する

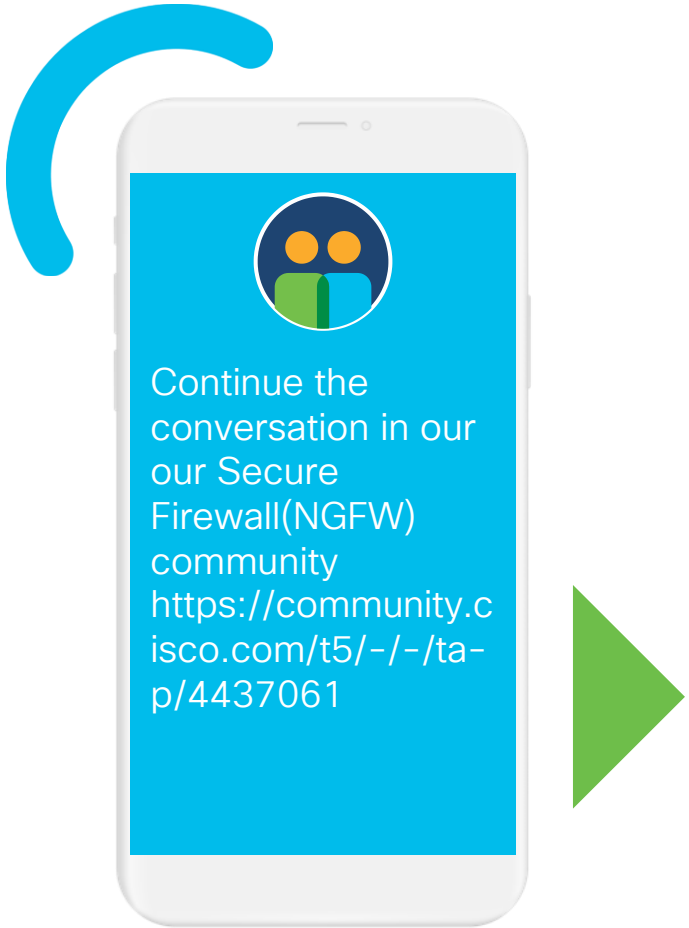
04 ベストプラクティスを確認して従う

Resources

Secure Firewall（NGFW）
ATXsリソースリンク集

https://community.cisco.com/t5/-/-/ta-p/4437061

※本日のATXs以外のリソースリンクも確認できます。




Cisco
Customer Experience