

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 コントロール 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

関連ポリシー

プレフィルタ

- トラフィックのファストパス / ドロップを事前に特定しパフォーマンスを向上
- トンネルルールの設定

セキュリティ インテリジェンス

Talos により提供される、または、カスタマイズされた URL / IP / DNS のグローバルブラックリスト

SSL / TLS

暗号化されたトラフィックをシステムがネットワーク上でどう対処するかを決定

基本条件

L2 - L4

- L2 (インターフェース / VLAN)
- L3 (IP / ポート)
- L4 (ポート)

高度な条件

アプリケーションの可視性

アプリケーションを特定しそのアプリケーションに関連するトラフィックに対するアクションを定義

アイデンティティ

ユーザを特定しそのユーザに関連するトラフィックに対するアクションを定義

URL

URLカテゴリまたは特定の URL に関連するトラフィックのブロックまたはアクセスを制限

検査

IPS

- Snort ルールベース
- ルールステートは3 :
 - Generate (イベント生成)
 - Drop and Generate (ドロップ及びイベント生成)
 - Disabled (無効)

高度な脅威

- ファイルに関連するトラフィックを対処
- 特定のファイルをブロックまたはファイル内のマルウェアを検出しブロック

アクション



信頼



許可



モニター



インタラクティブ
ブロック



ブロック

オブジェクト

ロギング

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

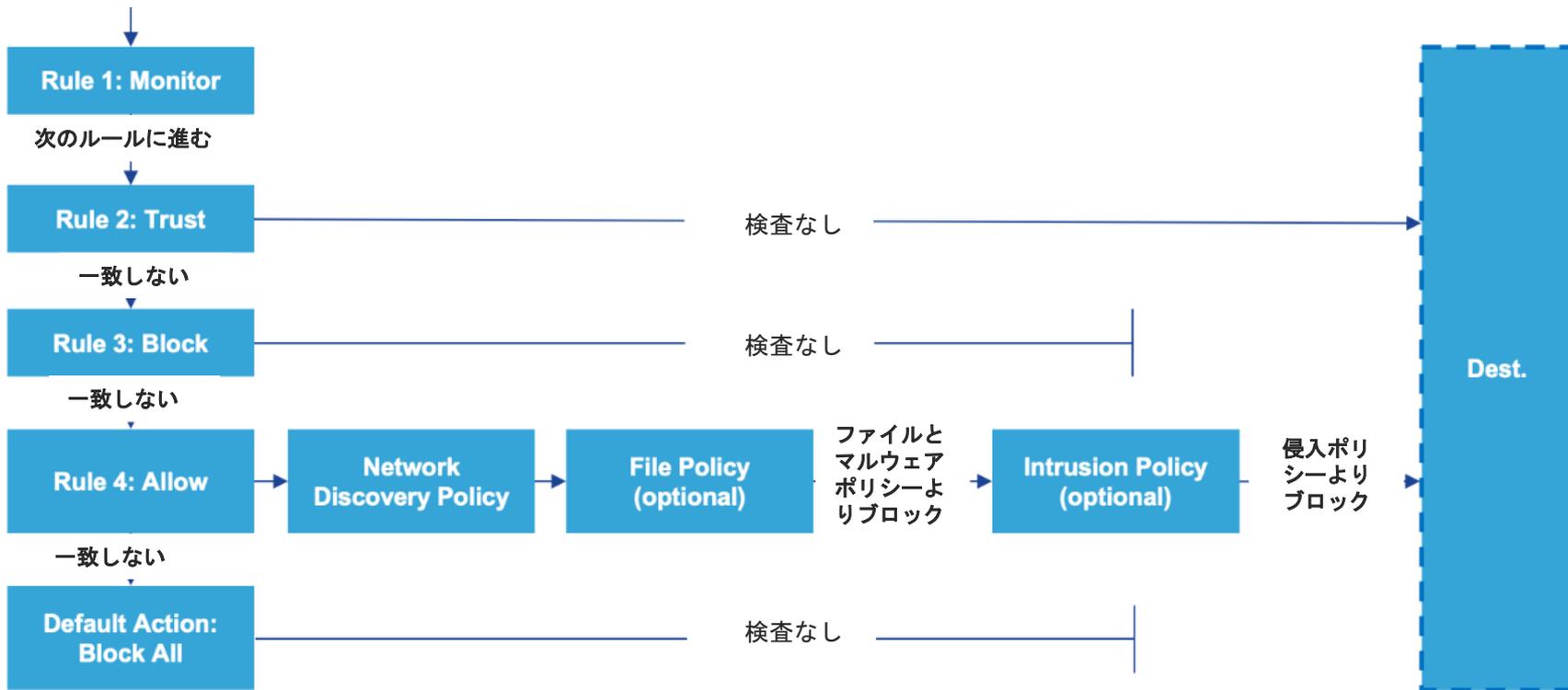
結果

信頼 (Trust)		トラフィックを即座にパス
許可 (Allow)		IPS / ファイルルールの検査
モニター (Monitor)		トラフィックのログのみ
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
ブロック (Block)		トラフィックのドロップ

	パス
	ドロップまたはパス
	パス
	パス
	ドロップ

アクセス コントロール ルールの処理

インバウンドパケット



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



- > AAA Server
- > Access List
- > Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- > Community List
- > Distinguished Name
- DNS Server Group
- > External Attributes
- File List
- > FlexConfig
- Geolocation
- Interface
- Key Chain

Interface

Interface objects segment your network to help you manage and classify traffic flow. An interface object can be configured on a single device.

Name ▲	Type
 Inside_Zone	Security Zone

オブジェクトタイプの概要



Firewall ポリシー



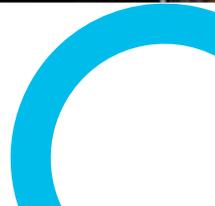
異なるポリシータイプの更新頻度は？

頻繁	時々	ほとんどない
<ul style="list-style-type: none">• アクセス コントロールポリシー• 侵入ポリシー	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

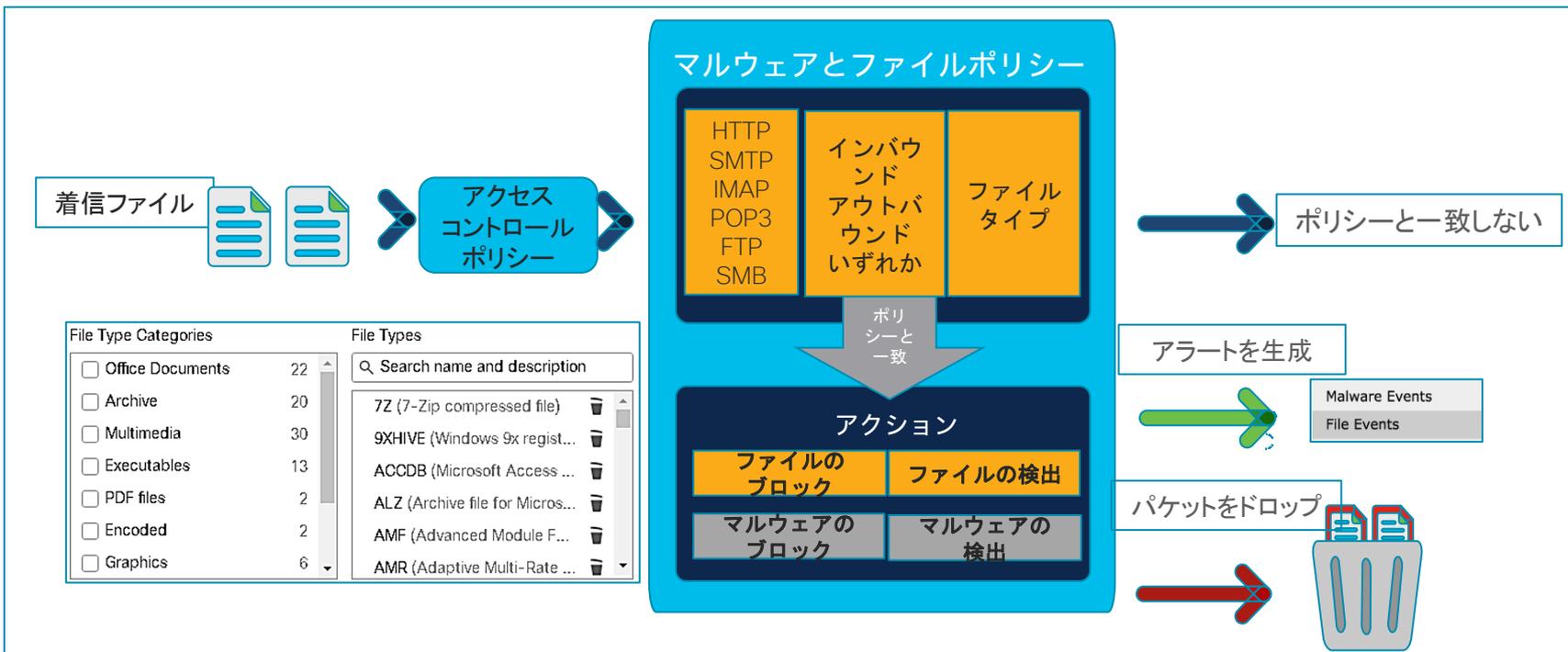
マルウェアとファイル ポリシー



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

Application Protocol

Any

Action

 Block Malware

Store Files

Malware

Unknown

Clean

Custom

Direction of Transfer

Any

Spero Analysis for MSEXEXE 1

Dynamic Analysis 2

Capacity Handling 1

Local Malware Analysis 3

Reset Connection

File Type Categories

<input type="checkbox"/> Office Documents	18
<input type="checkbox"/> Archive	19
<input type="checkbox"/> Multimedia	4
<input type="checkbox"/> Executables	10

File Types

Search name and description

7Z (7-Zip compressed file) 

ACCDB (Microsoft Access ...) 

ALZ (Archive file for Micros...) 

Add

Selected File Categories and Types

Category: System files	
Category: PDF files	
Category: Executables	
Category: Archive	

圧縮ファイルの検査

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

Archive File Inspection

Inspect Archives

Block Encrypted Archives

Block Uninspectable Archives

Max Archive Depth

Enter a value between 1 and 3

ファイルイベント



[Bookmark This Page](#) | [Reporting](#) | [Dashboards](#)

File Summary [\(switch workflow\)](#)

|| 2024-03-30 13:00

No Search Constraints ([Edit Search](#))

File Summary

Table View of File Events

Jump to...

<input type="checkbox"/>	↓ Time ×	Action ×	Sending IP ×	Sending Country ×	Receiving IP ×	Receiving Country ×	Sending Port ×	Receiving Port ×	SSL Status
▼ <input type="checkbox"/>	2024-03-30 14:58:01	Cloud Lookup Timeout	🌐 209.99.98.33	🇺🇸 USA	🖥️ 10.1.104.123		80 (http) / tcp	61376 / tcp	
▼ <input type="checkbox"/>	2024-03-30 14:53:54	Malware Cloud Lookup	🌐 54.231.252.202	🇺🇸 USA	🌐 10.1.120.26		80 (http) / tcp	61219 / tcp	
▼ <input type="checkbox"/>	2024-03-30 14:53:54	Malware Cloud Lookup	🌐 54.231.252.202	🇺🇸 USA	🌐 10.1.120.26		80 (http) / tcp	61248 / tcp	
▼ <input type="checkbox"/>	2024-03-30 14:49:55	Malware Cloud Lookup	🌐 23.9.102.155	🇨🇦 CAN	🖥️ 10.1.25.15		80 (http) / tcp	49195 / tcp	
▼ <input type="checkbox"/>	2024-03-30 14:47:46	Malware Cloud Lookup	🌐 54.231.252.210	🇺🇸 USA	🌐 10.1.115.42		80 (http) / tcp	62580 / tcp	
▼ <input type="checkbox"/>	2024-03-30 14:47:46	Malware Cloud Lookup	🌐 54.231.252.210	🇺🇸 USA	🌐 10.1.115.42		80 (http) / tcp	62621 / tcp	
▼ <input type="checkbox"/>	2024-03-30 14:42:24	Malware Cloud Lookup	🌐 174.35.24.67	🇺🇸 USA	🖥️ 10.1.62.22		80 (http) / tcp	59166 / tcp	
▼ <input type="checkbox"/>	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アトラジェクトリー



Firewall Management Center

Analysis / Files / Network File Trajectory

Overview

Analysis

Policies

Devices

Objects

Integration



Network File Trajectory for d2da2486...44b1f08e

File SHA256	d2da2486...44b1f08e   	First Seen	2021-06-09 14:21:33 on  185.43.223.164  jayda ball (dcloud.cisco.com/jball, LDAP)
File Name	term.xbel	Last Seen	2024-03-30 14:13:21 on  10.1.106.20 by
File Size (KB)	42.503	Event Count	9
File Type	SWF	Seen On	2 hosts
File Category	Multimedia	Seen On Breakdown	1 sender → 1 receiver
Current Disposition	 Malware 		
Threat Score	●●●● Very High		
Detection Name	SWF.Exploit.Kit.tht.VRT		

Trajectory



Events  Transfer  Block  Create  Move  Execute  Scan  Retrospective  Quarantine

Dispositions  Unknown  Malware  Clean  Custom  Unavailable

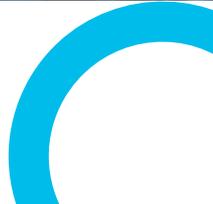
Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Dispositi	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



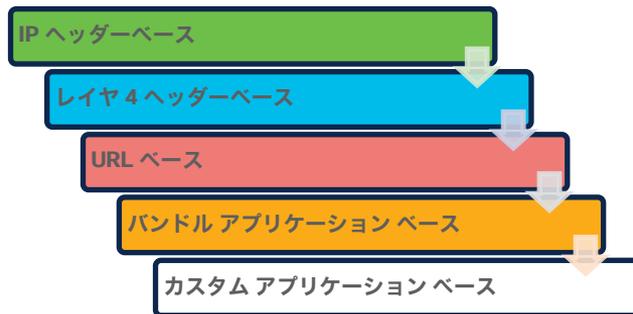
デモ： ファイルとマルウェア ポリシー

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、機器全体のパフォー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



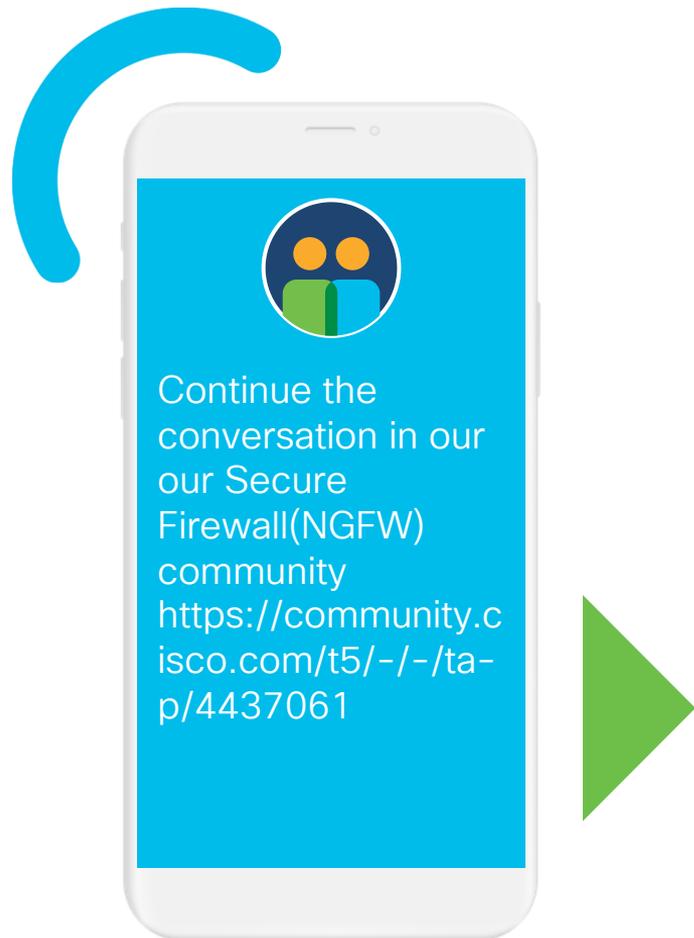
- 01 ACP のコンポーネントとパケットフローを理解する
- 02 パフォーマンスを最適化するために、最初から不要なファイルタイプをブロックする
- 03 マルウェアとファイル保護機能を有効にするために必要なライセンスがあることを確認する
- 04 ベストプラクティスを確認して従う

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