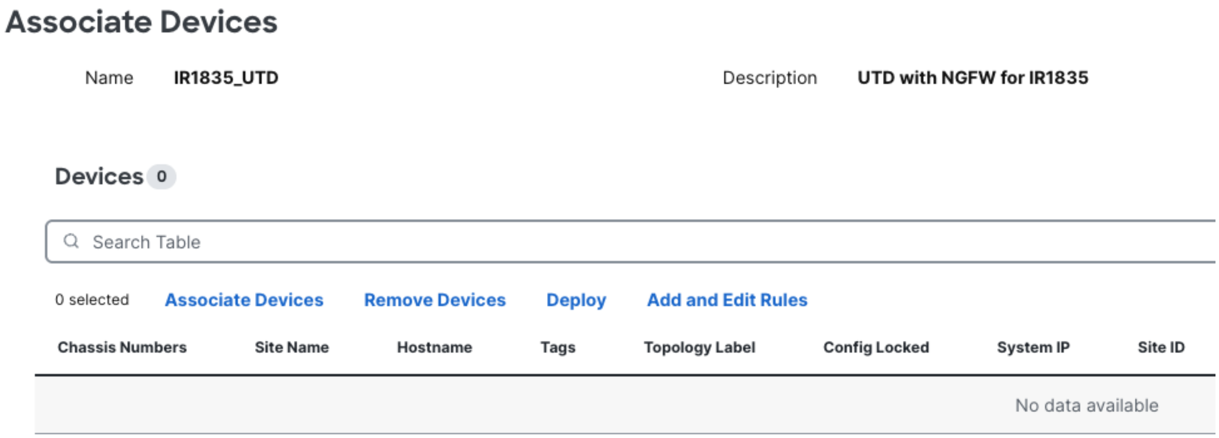
CVP: IR1835 SDWAN Policy Group with UTD (IPS/IDS/URL Filtering) and NGFW

Overview

This SD-WAN configuration is to be used to deploy Unified Thread Detection (UTD) application on IR1835. In addition to deploying the application, it also provides sample config for the Next Gen Fire Wall (NGFW) which enables the deployment of UTD as an app. It also includes sample configuration of the Advanced Inspection Profile witch can be further customized based on the use case.

Configuration Catalog Details

UTD is an IOX application which gets deployed on the IR1835 when the Policy Group is associated and deployed on the device which can be done in Policy Group -> Add:



Associate Devices

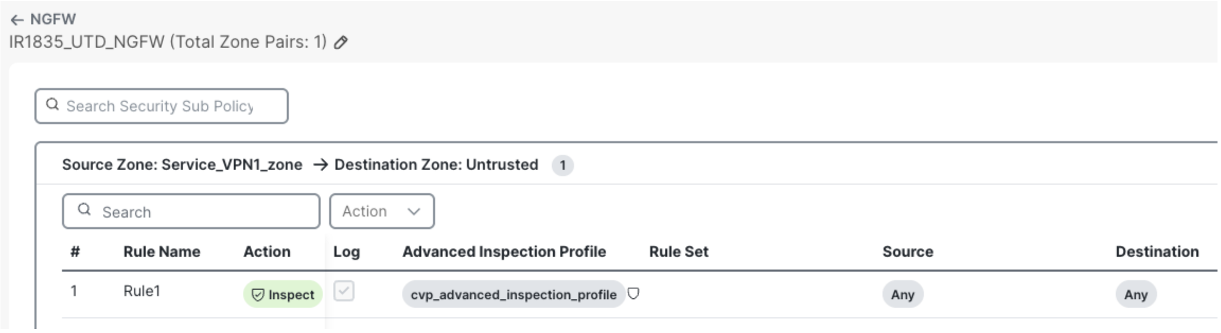
Name IR1835_UTD

Description UTD with NGFW for IR1835

Devices 0

Chassis Numbers	Site Name	Hostname	Tags	Topology Label	Config Locked	System IP	Site ID
						No data available	

When a Policy Group has a NGFW config which has at least one Inspect rule that calls for the Advanced Inspection Profile, that triggers the install of UTD on the IR1835 (example):



IR1835_UTD_NGFW (Total Zone Pairs: 1)

Source Zone: Service_VPN1_zone → Destination Zone: Untrusted 1

#	Rule Name	Action	Log	Advanced Inspection Profile	Rule Set	Source	Destination
1	Rule1	Inspect	✓	cvp_advanced_inspection_profile		Any	Any

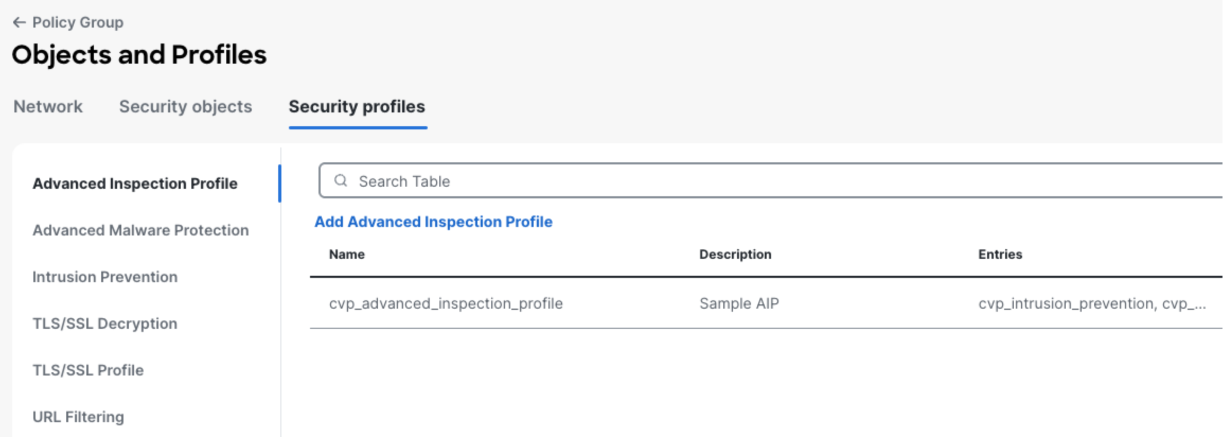
The NFGW can be very complicated or very simple to suit each use case. It is divided into Sub-Polices, each with multiple Rules. Each rule is applied to a source and destination

Cisco provides the configurations in this catalog as is for your convenience. These configurations have been built using industry best practices, observed across multiple deployments, which may be beneficial to you. Cisco is not responsible for any technical issues, bugs, or other issues that may arise from your use of these configurations and any resulting indirect, incidental, reliance, consequential, special or exemplary damages or loss of actual or anticipated revenue, profit, business, savings, data goodwill or use, business interruption, damaged data, wasted expenditure or delay in delivery (in all cases, whether direct or indirect).

Zone, hence the Zone Based Firewall (ZBFW). Zones can be defined in Configuration -> Policy Groups -> Objects and Profiles -> Security Objects -> Zones.

The Advanced Inspection Profile (AIP) once imported will be found in Configuration -> Policy Groups -> Objects and Profiles -> Security Profiles. The AIP calls all the other features supported by UTD. This is a sample list of features available within AIP and sample UI view:

- Advanced Malware Protection
- Intrusion Prevention
- TLS/SSL Decryption (Not supported on IR1835)
- TLS/SSL Profile (Not supported on IR1835)
- URL Filtering

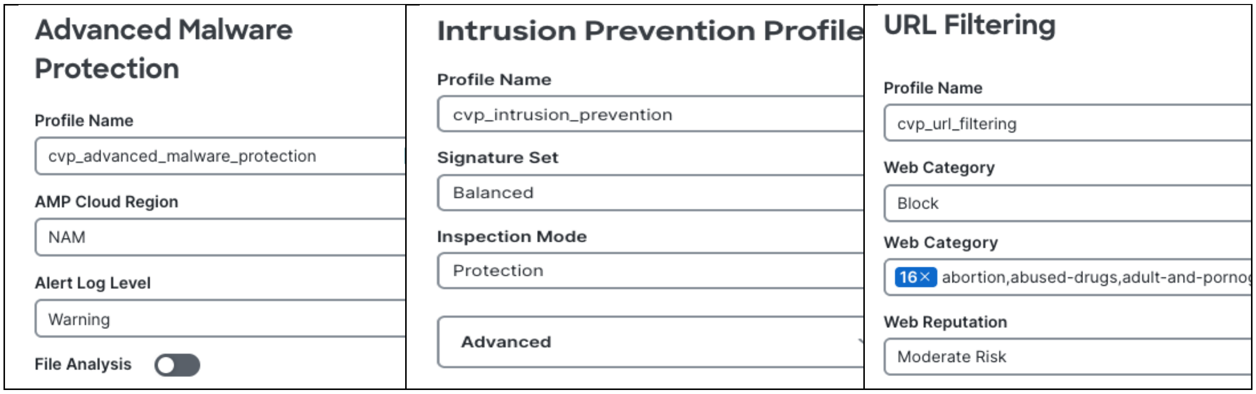


← Policy Group

Objects and Profiles

Name	Description	Entries
cvp_advanced_inspection_profile	Sample AIP	cvp_intrusion_prevention, cvp_...

Each of these profiles can be customized further as needed. For example, user can change the behavior of IPS and IDS or choose different categories of URLs to filter. User can also provide their own URLs to filter and chose the level of block. Likewise, they can also modify the Malware Protection further.



Advanced Malware Protection

Profile Name: cvp_advanced_malware_protection

AMP Cloud Region: NAM

Alert Log Level: Warning

File Analysis

Intrusion Prevention Profile

Profile Name: cvp_intrusion_prevention

Signature Set: Balanced

Inspection Mode: Protection

URL Filtering

Profile Name: cvp_url_filtering

Web Category: Block

Web Category: 16× abortion,abused-drugs,adult-and-pornog

Web Reputation: Moderate Risk

Cisco provides the configurations in this catalog as is for your convenience. These configurations have been built using industry best practices, observed across multiple deployments, which may be beneficial to you. Cisco is not responsible for any technical issues, bugs, or other issues that may arise from your use of these configurations and any resulting indirect, incidental, reliance, consequential, special or exemplary damages or loss of actual or anticipated revenue, profit, business, savings, data goodwill or use, business interruption, damaged data, wasted expenditure or delay in delivery (in all cases, whether direct or indirect).