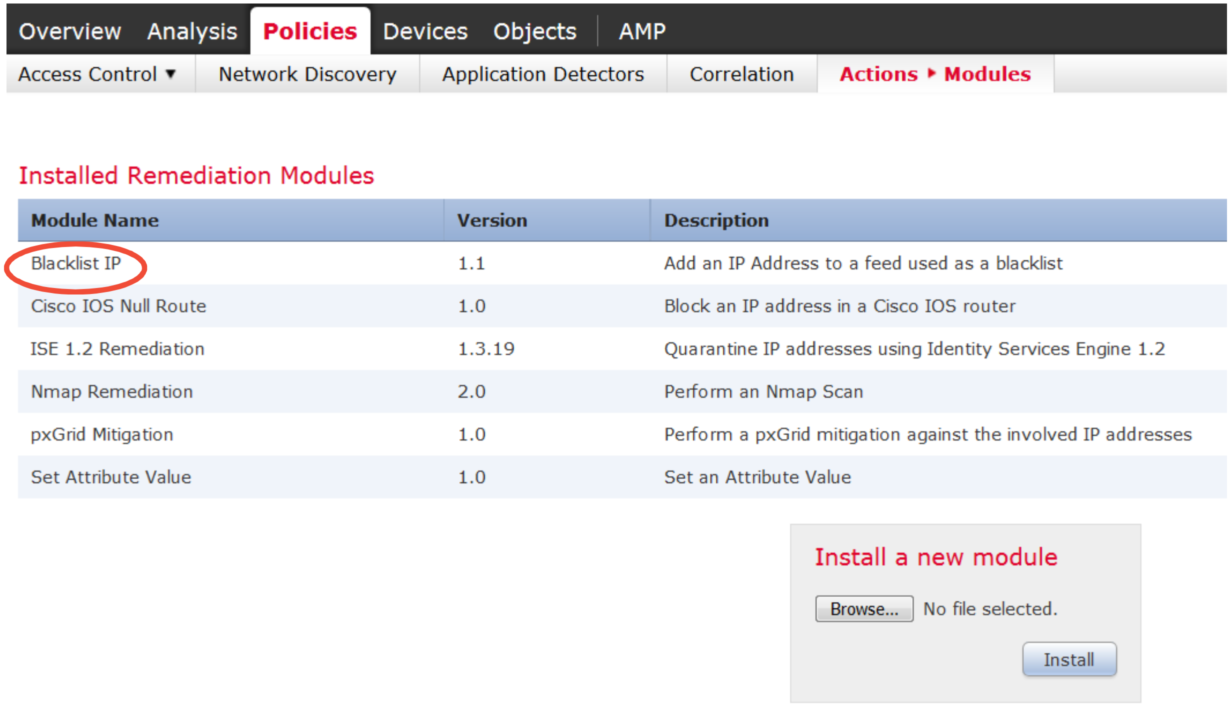
Custom Security Intelligence

- Correlate an action(s) with a remediation (in this case, create a custom security intelligence block list)
- In this example we are looking for blocking events based on geolocation and dropping the source IP into the custom security intelligence list.
- Monitor the events in Firepower Manager for a match against a rule.
- The remediation runs a perl script on the Firepower Manager, which leverages the remediation framework to parse event information.

Custom Security Intelligence



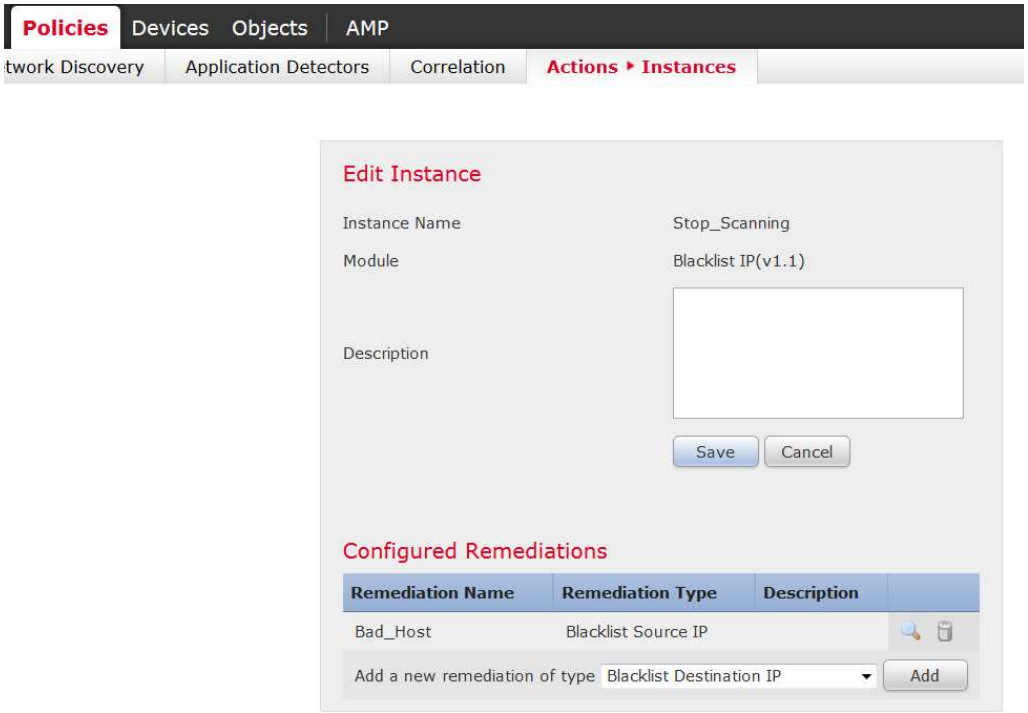
Installed Remediation Modules

Module Name	Version	Description
Blacklist IP	1.1	Add an IP Address to a feed used as a blacklist
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
ISE 1.2 Remediation	1.3.19	Quarantine IP addresses using Identity Services Engine 1.2
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value

Install a new module

Browse... No file selected.

Custom Security Intelligence



Edit Instance

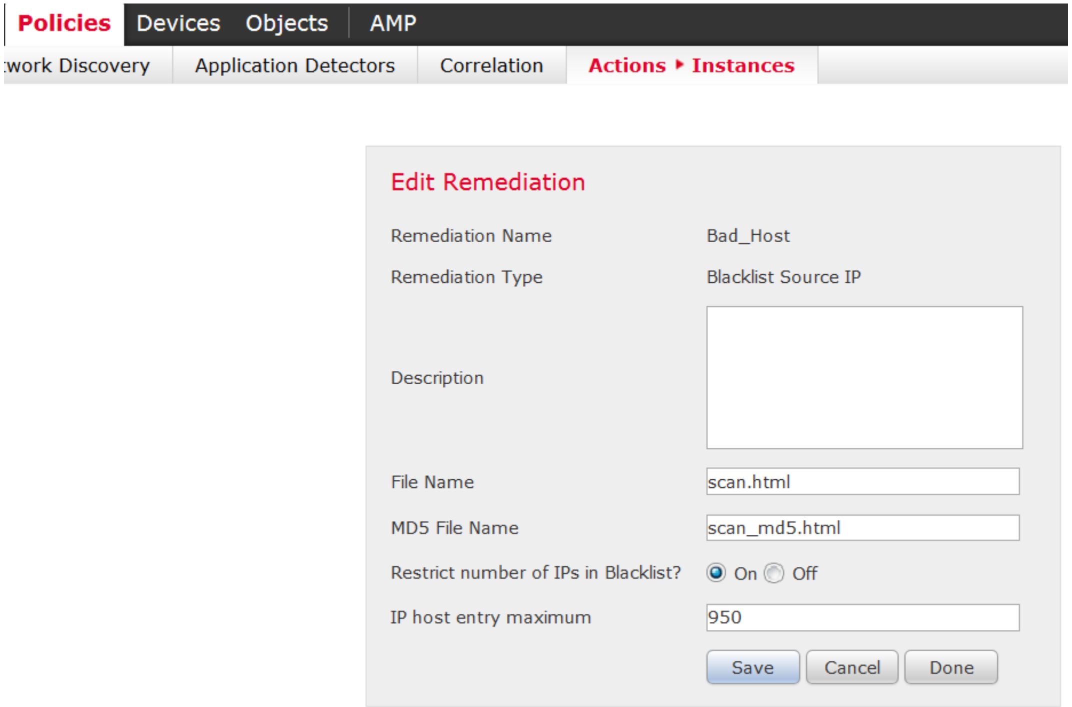
Instance Name	Stop_Scanning
Module	Blacklist IP(v1.1)
Description	

Configured Remediations

Remediation Name	Remediation Type	Description	
Bad_Host	Blacklist Source IP		

Add a new remediation of type Blacklist Destination IP

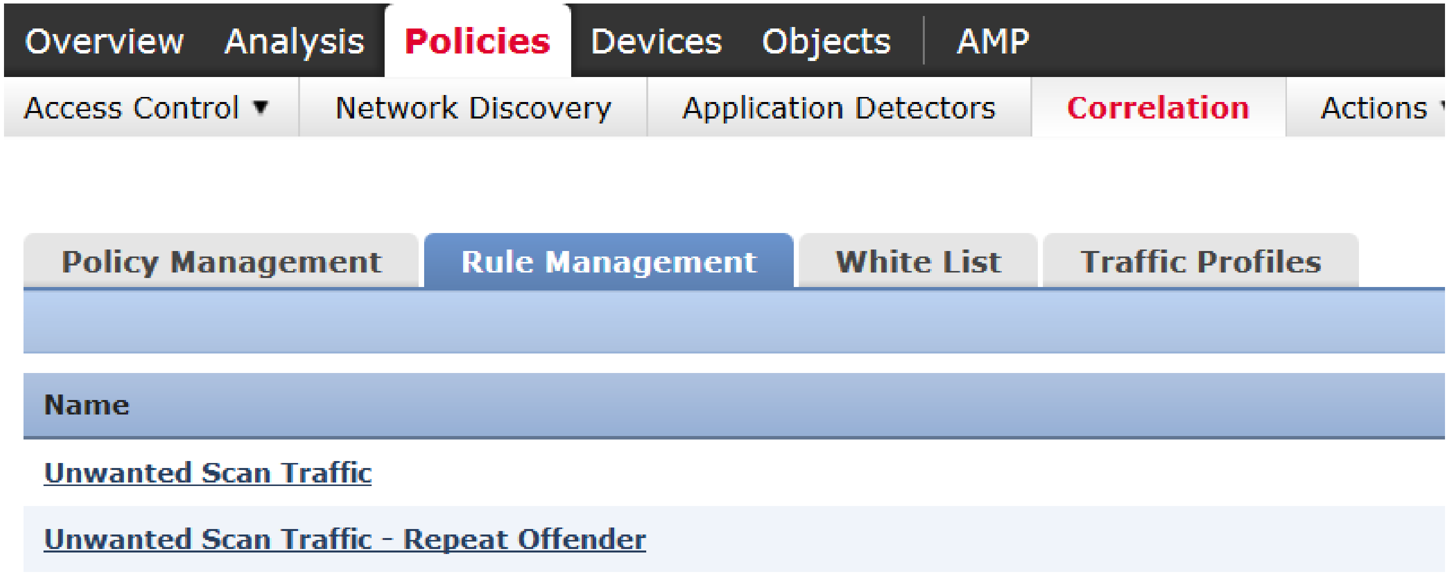
Custom Security Intelligence



Edit Remediation

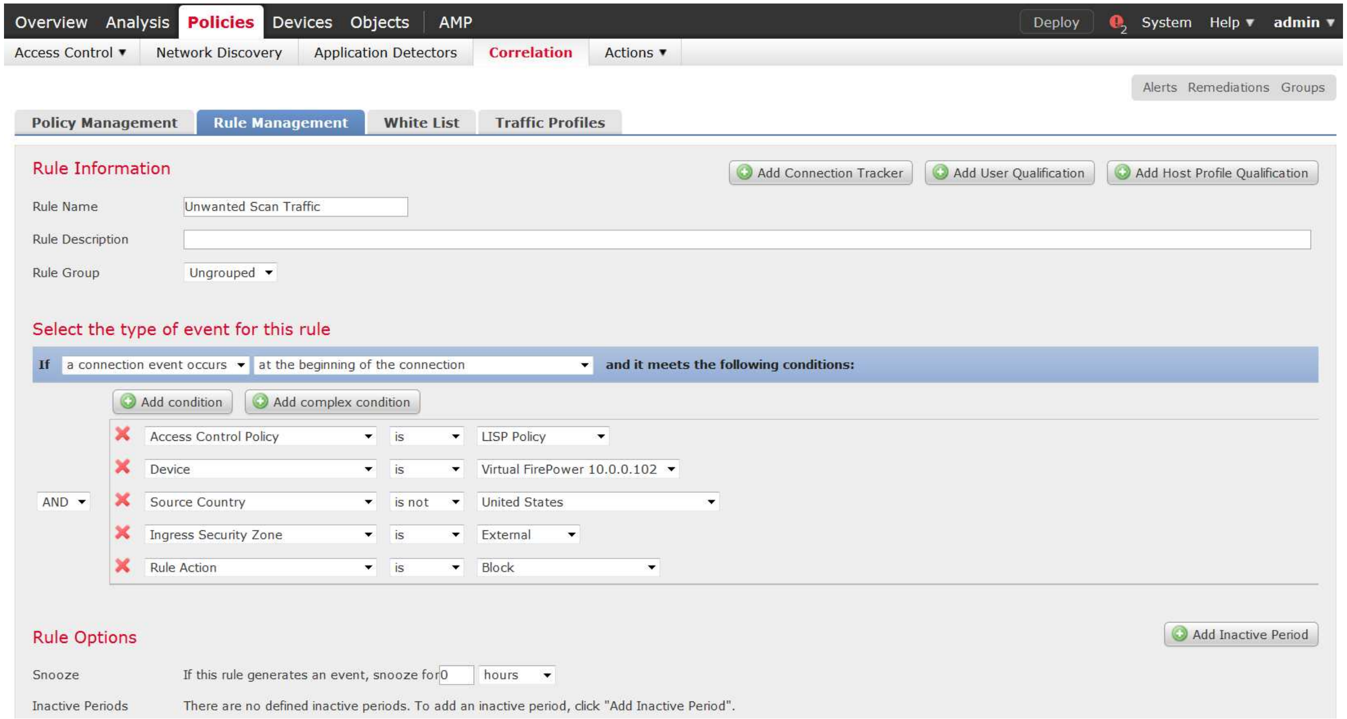
Remediation Name	Bad_Host
Remediation Type	Blacklist Source IP
Description	
File Name	scan.html
MD5 File Name	scan_md5.html
Restrict number of IPs in Blacklist?	● On ○ Off
IP host entry maximum	950

Custom Security Intelligence



Name
Unwanted Scan Traffic
Unwanted Scan Traffic - Repeat Offender

Custom Security Intelligence



Rule Information

Rule Name	Unwanted Scan Traffic
Rule Description	
Rule Group	Ungrouped

Select the type of event for this rule

If a connection event occurs at the beginning of the connection and it meets the following conditions:

AND

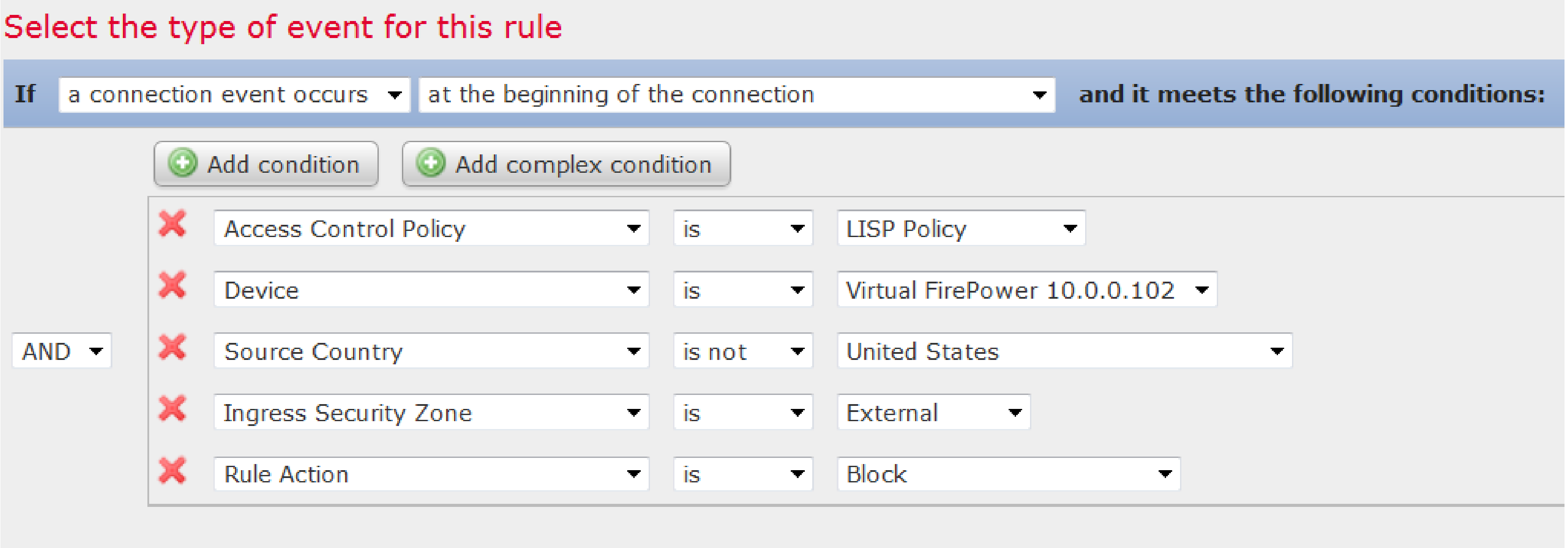
Access Control Policy	is	LISP Policy
Device	is	Virtual FirePower 10.0.0.102
Source Country	is not	United States
Ingress Security Zone	is	External
Rule Action	is	Block

Rule Options

Snooze: If this rule generates an event, snooze for 0 hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Custom Security Intelligence

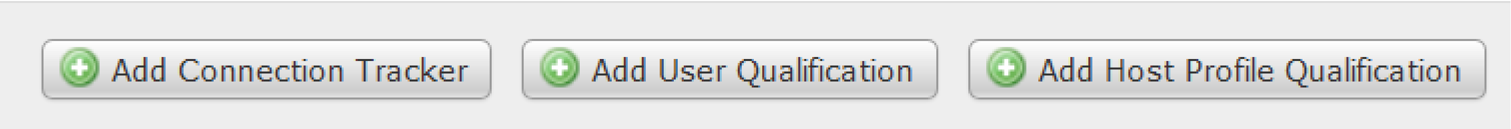


Select the type of event for this rule

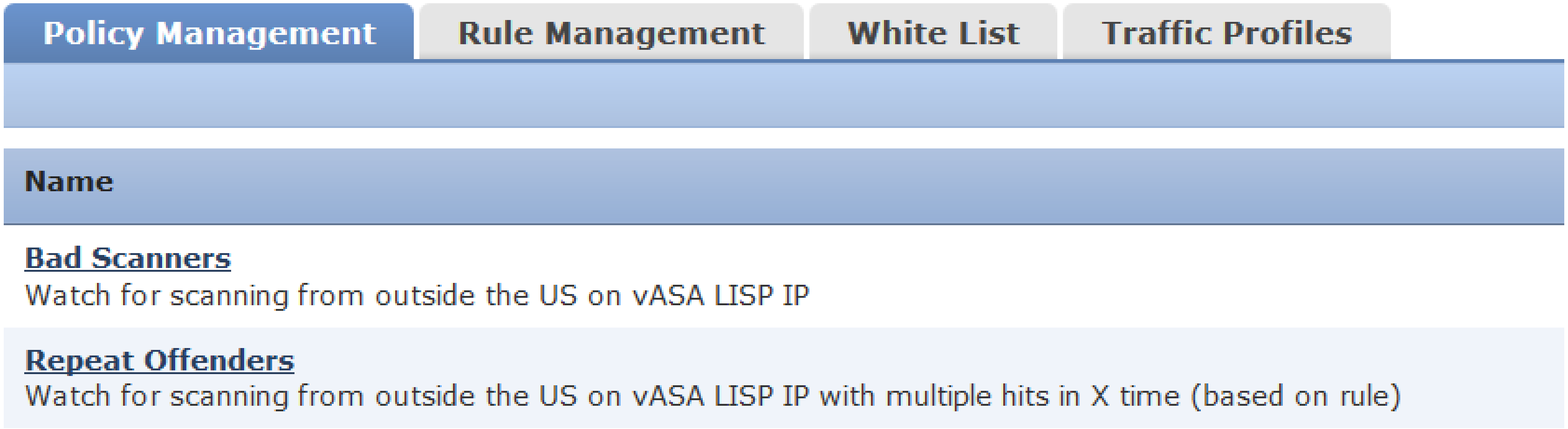
If a connection event occurs at the beginning of the connection and it meets the following conditions:

AND

Access Control Policy	is	LISP Policy
Device	is	Virtual FirePower 10.0.0.102
Source Country	is not	United States
Ingress Security Zone	is	External
Rule Action	is	Block

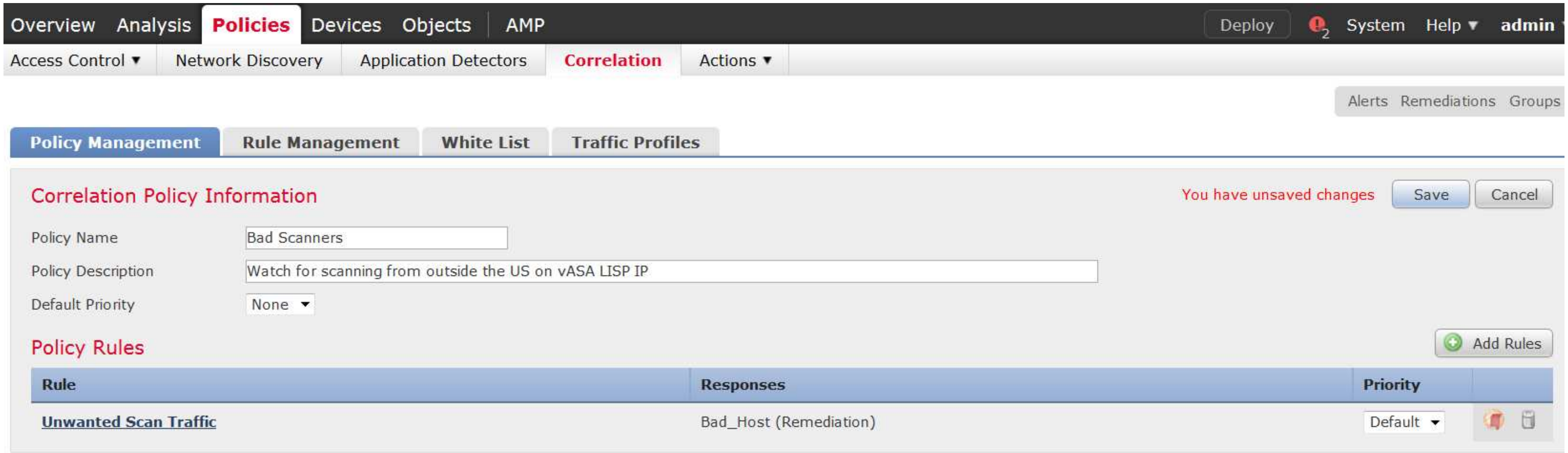


Custom Security Intelligence



Name
Bad Scanners Watch for scanning from outside the US on vASA LISP IP
Repeat Offenders Watch for scanning from outside the US on vASA LISP IP with multiple hits in X time (based on rule)

Custom Security Intelligence



Correlation Policy Information

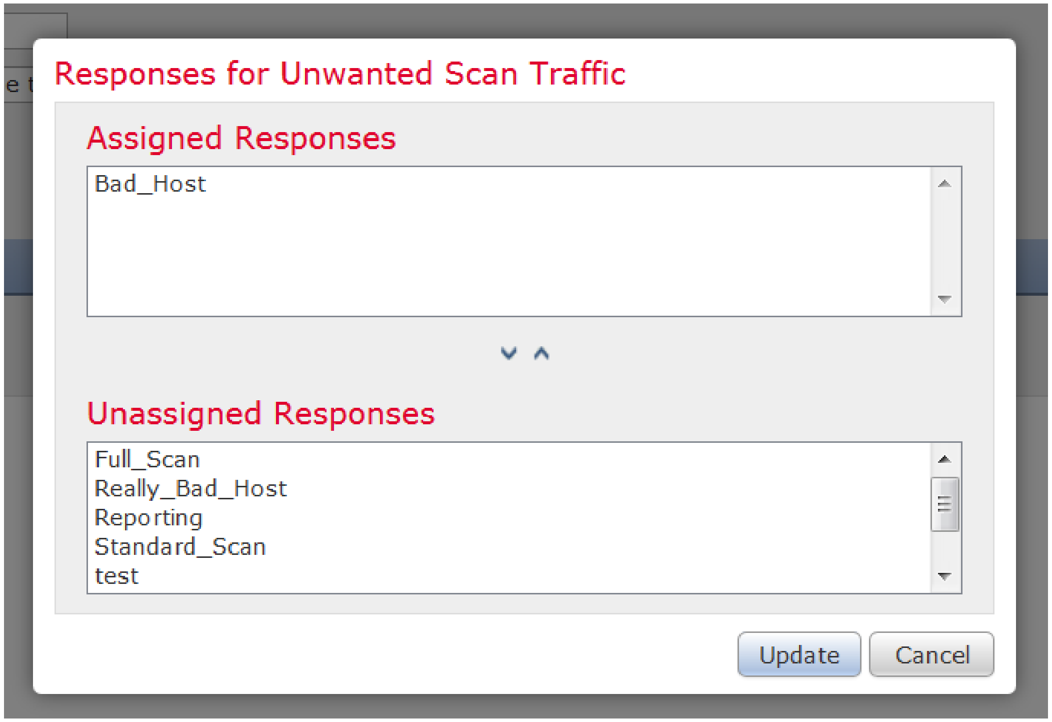
You have unsaved changes

Policy Name	Bad Scanners
Policy Description	Watch for scanning from outside the US on vASA LISP IP
Default Priority	None

Policy Rules

Rule	Responses	Priority
Unwanted Scan Traffic	Bad_Host (Remediation)	Default

Custom Security Intelligence



Responses for Unwanted Scan Traffic

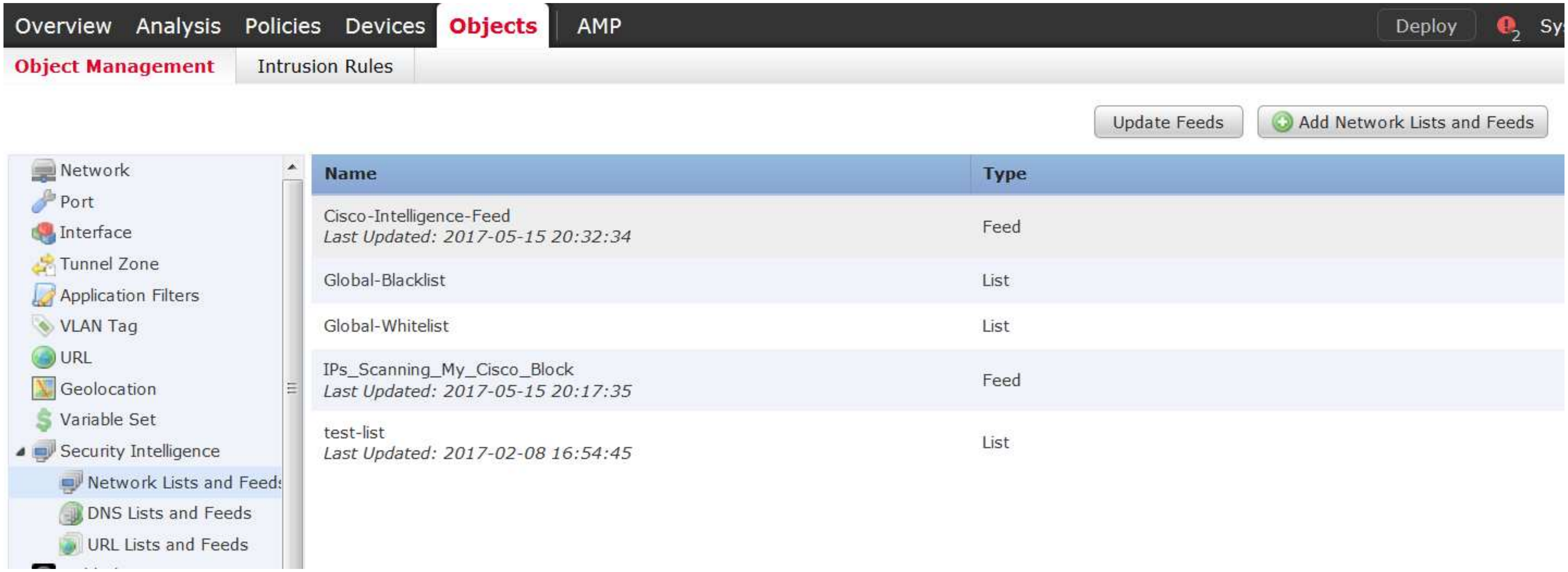
Assigned Responses

Bad_Host

Unassigned Responses

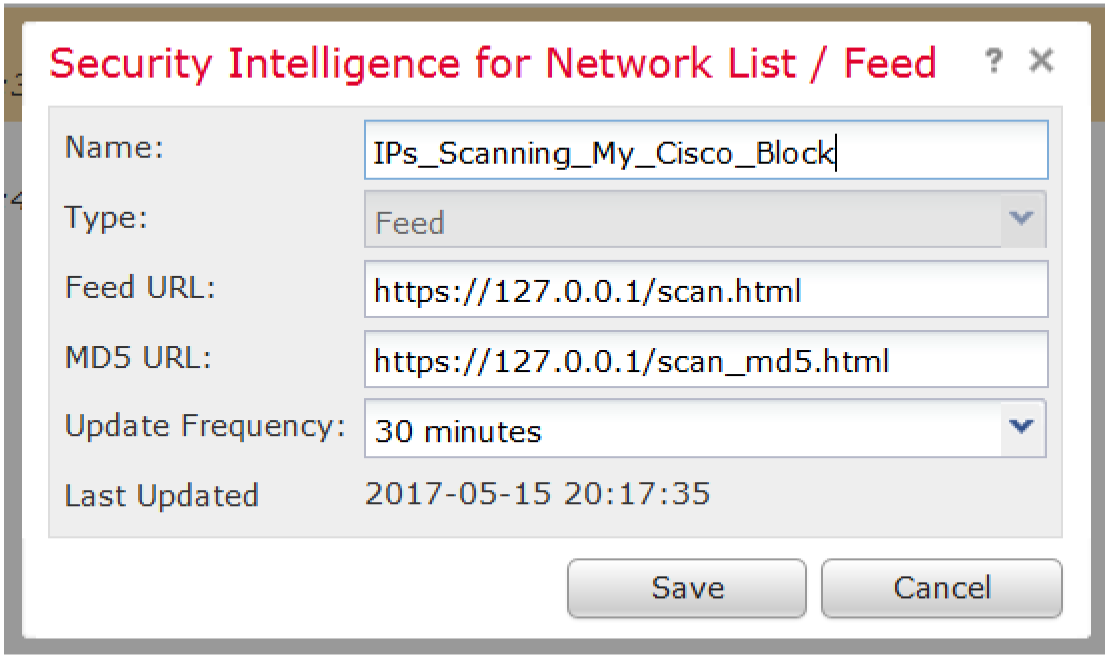
Full_Scan
Really_Bad_Host
Reporting
Standard_Scan
test

Custom Security Intelligence



Name	Type
Cisco-Intelligence-Feed *Last Updated: 2017-05-15 20:32:34*	Feed
Global-Blacklist	List
Global-Whitelist	List
IPs_Scanning_My_Cisco_Block *Last Updated: 2017-05-15 20:17:35*	Feed
test-list *Last Updated: 2017-02-08 16:54:45*	List

Custom Security Intelligence



Security Intelligence for Network List / Feed

Name:	IPs_Scanning_My_Cisco_Block
Type:	Feed
Feed URL:	https://127.0.0.1/scan.html
MD5 URL:	https://127.0.0.1/scan_md5.html
Update Frequency:	30 minutes
Last Updated	2017-05-15 20:17:35

Reference Material