



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Implementing and Auditing CIS Controls (Security 566)"
at <http://www.giac.org/registration/gccc>

Know Thy Network - Cisco Firepower and Critical Security Controls 1 & 2

GIAC (GCCC) Gold Certification

Author: Ryan Firth, RyanQFirth+gccc@gmail.com

Advisor: Rob VandenBrink

Accepted: 9/16/2016

Abstract

Previously known as the SANS Top 20, the Critical Security Controls are based on real-world attack and breach data from around the world; they are objectively the most effective technical controls against known cyber-attacks. Due to competing priorities and demands, however, organizations may not have the expertise to figure out how to implement and operationalize the Critical Security Controls in their environments. This paper will help bridge that gap for security and network teams using Cisco Firepower.

Cisco Systems is one of the world's largest cybersecurity companies. Their Next-Generation Firewalls, IPS, and Firepower Management Center are key products in their security portfolio. This paper will walk through the implementation of several recommendations from the Critical Security Controls 6.0 in the Cisco Firepower Management Center (FMC) platform, formerly known as FireSIGHT and Sourcefire Defense Center. FMC 6.0.1 with Firepower Threat Defense 6.0.1 are used in configuration examples.

See Appendix-A for a quick reference guide to this document

1. Introduction

Originally conceived in 2008 in an effort by the NSA to assist the Department of Defense in prioritizing its cybersecurity spending, the Critical Security Controls (CSC) are based on the principle that “offense must inform defense.” Hundreds of IT and security organizations experienced in cybersecurity, attack development, and breach response have contributed in a public-private consortium to produce a prioritized list of the most effective cybersecurity controls. Based on actual attack data from intelligence agencies and cybersecurity companies around the world, this effort resulted in the first “20 Critical Controls,” released by the Commission on Cybersecurity. These controls evolved into the popular “SANS Top 20” before reaching its current home with the Center for Internet Security (CIS).

From *The CIS Critical Security Controls for Effective Cyber Defense*, version 6.0:

The CIS Critical Security Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. (CIS, 2015)

Cisco Firepower is a combination Next-Generation Intrusion Prevention System (NGIPS) and Next-Generation Firewall (NGFW). Gartner helped to popularize the term NGFW, summarizing it as “deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.” (Gartner, 2016) Engineers familiar with Cisco Firepower may not be aware of the detailed recommendations contained in the Critical Security Controls, or their effectiveness.

Author Name, email@addressgmail.com

Conversely, those familiar with the Critical Security Controls may not have the firewall and IPS skills necessary to implement the controls. Security practitioners are left to bridge these gaps on their own.

1.1. Critical Security Controls 1 & 2

The first two critical controls are best summarized in the commandment “Know thy network.” Control 1 (Inventory of Authorized and Unauthorized Devices) focuses on tracking what devices are connected to a network at any given time, tying that information back to an inventory control system, and taking action on unauthorized devices. The description of CSC 1 is as follows: “Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.” (CIS, 2015)

DHCP logging, establishing automated acquisition processes, utilizing 802.1x for access control, and client certificates are some of the recommendations found in the first control and its six sub-controls. The promise of the “Internet of Things” (IoT) to bring far more diversity and insecurity to the endpoint makes Control 1 more difficult—and necessary—than ever before.

While Control 1 can be incredibly difficult to operationalize, Control 2 and its four sub-controls is at least as challenging. Maintaining an “Inventory of Authorized and Unauthorized Software,” as defined by Control 2 requires many techniques, such as file integrity checking, application whitelisting, software inventory systems, and virtualization to name a few. Organizations are at the mercy of operating system and software vendors, along with all their unique quirks, to maintain appropriate controls. The description of CSC 2 states, “Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.” (CIS, 2015)

No single product can fully implement the Critical Security Controls in its entirety, in part due to the diversity of recommendations, and partly due to the inclusion of process-oriented and other items not addressable by a product. While some sub-

controls are easily implemented in Firepower, others are far outside the scope of the product. This paper will walk through examples of operationalizing some or all of the following sub-controls from *The CIS Critical Security Controls for Effective Cyber Defense*, version 6.0:

Sub-control 1.1:

Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to the organization's public and private network(s). Active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

Sub-control 1.4:

Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

Sub-control 2.3:

Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

Cisco ISE (Identity Services Engine), paired with the host posturing features of the Cisco AnyConnect client, provide greater host visibility and network access control capabilities. By combining Firepower, ISE, and AnyConnect, an organization can adhere to all six sub-controls of Critical Control 1, and much of Critical Control 2.

2. Implementation of the Controls

Establishing effective security controls takes time, patience, and perseverance. In a network containing hundreds or thousands of devices scattered globally, perhaps both on-premises and in co-location or IaaS environments, implementing new security controls may be a daunting task. Adding in corporate politics, competing agendas, and a rainbow of personalities may make success seem impossible. To the overwhelmed security professional, the advice “don’t try to boil the ocean” is highly relevant.

Following recommendations from the Project Management Institute’s *PMBOK Guide*, developing a project charter, identifying the stakeholders, and obtaining their buy-in should be completed at the start of a new security controls project.

Testing new security controls in a non-production environment and identifying business risks associated with these changes is also highly recommended. Ideally, plan to implement these controls first within a low-risk, well-defined environment in case unexpected complications arise.

Implementors should tweak processes as the environment requires, making sure to document well along the way—especially areas where exceptions must be made. Recommending compensating controls for those exceptions may be required to reduce risk to an acceptable level. Prioritizing the organization’s most critical assets early in the project, but after testing and the initial rollout, should also be considered. Not only is the security posture of those assets strengthened first, but they will already have been addressed if the project is delayed or canceled halfway through.

2.1. A warning about implementation

Cisco Firepower devices offer flexible configuration options and are installed in a wide variety of environments. Recommendations in this guide are acceptable for most environments; however, engineers should first understand the impact of any change prior to implementation. This document does not reflect the opinion or recommendations of

Cisco Systems unless specifically referenced. By utilizing the guidance contained in this document, you assume total responsibility for the consequences. The author, contributors, and Cisco Systems are not liable for any damages incurred directly or indirectly from the use of this document.

2.2. Implementing discovery

Knowing what applications and devices exist on the network is a core focus of the first two Critical Security Controls. An organization must be able to effectively compare the difference between what *should* exist, and what *actually* exists. This requires both a well-documented, up-to-date inventory of approved applications and devices, (what *should* exist) and a method of effective discovery (what *actually* exists). Firepower offers several methods to provide the latter.

Implementation at-a-glance:	<ol style="list-style-type: none"> 1. Enable passive inventory discovery <ol style="list-style-type: none"> i. Create an object for your organization's public IP space ii. Create a Network Discovery policy for private IP addresses iii. Create a Network Discovery policy for public addresses where inventory is desired iv. Deploy the configuration to managed devices 2. Enable scheduled Nmap scanning <ol style="list-style-type: none"> v. Create an Nmap Remediation instance vi. Create an Nmap Remediation policy for scheduled scanning vii. Create the scan target, specifying which networks Nmap should scan regularly viii. Schedule the Nmap scan 3. Enable automated scanning of new hosts <ol style="list-style-type: none"> ix. Create a Correlation Rule for detecting new
-----------------------------	---

	<p>IP hosts</p> <p>x. Create a Correlation Policy to trigger scanning</p> <p>4. Viewing discovery information</p>
--	---

2.2.1. Enable passive inventory discovery

The Firepower System can discover hosts, services, and users by passively inspecting traffic as it flows through a Firepower device. Host profiles are automatically created for discovered hosts, and contain information about the operating system, listening services, network applications in use, user history, indicators of compromise, vulnerabilities, and other attributes. By building an inventory passively, new hosts and services are known in real-time. Passive discovery is especially useful for networks where active scanning poses too much risk to operations, such as in the case of many SCADA, IoT, Operational Technology (OT), or critical infrastructure environments.

It is important to consider the placement of Firepower devices in a network when relying heavily on passive network discovery. The Firepower system cannot passively detect a host whose traffic does not traverse a Firepower device. In the case of a remote office with a direct Internet connection, instead of backhauled through a data center, a Firepower device at the data center may not see any traffic from hosts at the remote office. Utilizing Firepower's Nmap scanning feature or collecting NetFlow information from remote devices can mitigate this risk.

- i. Create an object for your organization's public IP space:
 - a. In FMC, navigate to *Objects > Object Management > Network*
 - b. Click *Add Network > Add Object*
 - c. Create a name, e.g. **CompanyX-Public-Austin**
 - d. Input the subnets or IPs that Firepower should analyze, then click Save

- e. (Optional) For multiple public subnets, Click *Add Network > Add Group* to combine multiple address objects into a single object.

- ii. Create a Network Discovery policy for private IP addresses:
 - a. In FMC, navigate to *Policies > Network Discovery > Networks*
 - b. Click *Add Rule*
 - c. Under *Available Networks* select *IPv4-Private-All-RFC1918* then click *Add*

Note: Add private and local IPv6 addresses if utilized and desired for inventory.

- d. Click the *Zones* tab
- e. Select the appropriate zones where RFC 1918 addresses should reside within the network and click *Add* (Zone specification is optional but recommended for performance)

- f. Ensure *Action:* is set to *Discover* and the *Hosts* box is checked, then click *Save* (Discovering *Users* may also be desired)

Networks Users Advanced					Add Rule	
Networks	Zones	Source Port Exclusion...	Destination Port Exclusion...	Action		
IPv4-Private-All-RFC191	Inline-Inside (Inline)	none	none	Discover: Hosts, Users		

- iii. Create a Network Discovery policy for public addresses where inventory is desired:
 - a. In FMC, navigate to *Policies > Network Discovery > Networks*
 - b. Click *Add Rule*
 - c. Under *Available Networks* select the object(s) created in step i.c. or i.e. above, e.g. **CompanyX-Public-All**, then click *Add*
 - d. Click the *Zones* tab
 - e. Select the appropriate zones where the public IP addresses should reside on the network and click *Add* (Zone specification is optional for performance)
 - f. Ensure *Action:* is set to *Discover* and the *Hosts* box is checked, then click *Save* (Discovering *Users* may not be desired here)

Networks Users Advanced					Add Rule	
Networks	Zones	Source Port Exclusion...	Destination Port Exclusion...	Action		
CompanyX-Public-All	Inline-Outside (Inline)	none	none	Discover: Hosts, Applic		

- iv. Deploy the configuration to managed devices:
 - a. From the main FMC page, click *Deploy*
 - b. Select the appropriate devices, then click the *Deploy* button.

2.2.2. Enable scheduled Nmap scanning

Although configuring Firepower to passively discover hosts and services allows for real-time detection, there is a limit to how much information can be inferred about a host through traffic inspection. Actively scanning hosts with the built-in Nmap scanner can help Firepower build a more complete and accurate host profile.

Tip: Accurately detecting new operating systems and services requires regular signature updates. It is highly recommended to schedule Firepower to both download and install new Vulnerability Database (VDB) signatures on a regular basis. See the Firepower Management Center Configuration Guide under “Task Scheduling” for details.

IPS rules are enabled based on the operating system and services running on a host. Scheduled Nmap scans help ensure that the most relevant IPS rules are enabled. Host information gathered through Nmap scanning is not overridden through passive discovery, therefore it is important to schedule regular, automated Nmap scans. Alternatively, Firepower can also obtain host information via third-party data.

- v. Create an Nmap Remediation instance:
 - a. Choose *Policies > Actions > Instances*
 - b. Select a module type of *Nmap Remediation*
 - c. If this Nmap instance should not scan a host or network, specify their IP address or subnet under *Black Listed Scan hosts*.
 - d. If scanning from a remote Firepower device is desired, instead of scanning from the Firepower Management Center (FMC), specify the device name in the *Remote Device Name* field.

Note: For distributed environments, especially those where high latency exists between the FMC and subnets to be scanned, it is highly recommended to use the remote Firepower device for scanning. Create a separate Nmap instance for each remote location with a Firepower device.

- e. Provide a unique name for the instance, e.g. **Nmap-Inst-Austin** and click *Create*
- f. Select *Nmap Scan*, then click *Add*

The screenshot shows the 'Edit Instance' configuration page in the Cisco Firepower Management Center. The page has a navigation bar at the top with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Deploy, System, Help, and admin. Below the navigation bar are sub-tabs for Access Control, Network Discovery, Application Detectors, Correlation, and Actions > Instances. The main content area is titled 'Edit Instance' and contains the following fields:

- Instance Name: Nmap-Inst-Austin
- Module: Nmap Remediation(v2.0)
- Description: (empty text area)
- Black Listed Scan hosts (an optional list of networks): (empty text area)
- Remote Device Name (optional): Austin-5508

Below the fields are 'Save' and 'Cancel' buttons. At the bottom, there is a 'Configured Remediations' section with a table header (Remediation Name, Remediation Type, Description) and a message 'No configured remediations available'. Below this is a button to 'Add a new remediation of type' with a dropdown menu showing 'Nmap Scan' and an 'Add' button.

- vi. Create an Nmap remediation policy for scheduled scanning
 - a. Provide a unique remediation name, e.g. **Nmap-Remed-Austin**
 - b. Scan Which Address(es) From Event?: *Scan Source Address Only*
 - c. Scan Type: *TCP Syn Scan*
 - d. Scan for UDP ports: *Off* (UDP scanning dramatically increases scan time, and is not recommended unless specifically required)
 - e. Use Port From Event: *Off*

- f. Scan from reporting device: *Off*
- g. Fast Port Scan: *Off*
- h. Port Ranges and Scan Order: Leave blank

Note: Nmap scans 1,000 common ports by default. For a comprehensive scan of all TCP ports, specify 1-65535. Network size, reliability, types of hosts, scan window, and performance are some of the main concerns of performing a full port scan.

- i. Probe open ports for vendor and version information: *On*
- j. Service Version Intensity: *7*
- k. Detect Operating System: *On*
- l. Treat All Hosts As Online: *On*
- m. Host Discovery Method: *TCP SYN*
- n. Host Discovery Port List: Leave blank
- o. Default NSE Scripts: *On*
- p. Timing Template: *3*

Edit Remediation

Remediation Name: Nmap-Remed-Austin

Remediation Type: Nmap Scan

Description: [Empty text area]

Scan Which Address(es) From Event? Scan Source Address Only

Scan Type: TCP Syn Scan

Scan for UDP ports: ☐ On ☒ Off

Use Port From Event: ☐ On ☒ Off

Scan from reporting device: ☐ On ☒ Off

Fast Port Scan: ☐ On ☒ Off

Port Ranges and Scan Order (blank for Nmap defaults): [Empty text field]

Probe open ports for vendor and version information: ☒ On ☐ Off

Service Version Intensity: 7

Detect Operating System: ☒ On ☐ Off

Treat All Hosts As Online: ☒ On ☐ Off

Host Discovery Method: TCP SYN

Host Discovery Port List (advanced option): [Empty text field]

Default NSE scripts: ☒ On ☐ Off

Timing Template (Higher Is Faster): 3

[Create] [Cancel]

- vii. Create the scan target, specifying which networks Nmap should scan regularly

Note: Create multiple Targets for each IP Range you wish to scan on a different schedule or with a different scanning device.

- Choose *Policies > Actions > Scanners*
- Click *Targets*
- Click *Create Scan Target*
- Provide a name for the scan, e.g. **Austin-DMZ**

- e. Enter the IP Ranges desired for scanning
- f. Delete any ports listed, leaving the *Ports* field blank, and click *Save*

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies' (selected), 'Devices', 'Objects', 'AMP', 'Deploy', 'System', 'Help', and 'admin'. Below this, a secondary bar shows 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions > Scanners'. A sub-menu for 'Scanners' is open, showing 'Scanners', 'Scan Results', 'Targets', and 'Import Results'. The 'Target Information' dialog box is centered, with the following fields: 'Name' (Austin-DMZ), 'IP Range' (10.10.0.0/16), and 'Ports' (empty). 'Save' and 'Cancel' buttons are at the bottom of the dialog.

- viii. Schedule the Nmap scan
 - a. Navigate to *System > Tools > Scheduling*
 - b. Click *Add Task*
 - c. Job Type: *Nmap Scan*
 - d. Scheduled task to run: *Recurring*
 - e. Schedule the task to run at a time and day acceptable to the organization. Frequently scanning the environment will provide a more up-to-date and accurate inventory. Scanning once per day is recommended for many environments, however, this setting is highly environment-dependent.
 - f. Nmap Remediation: Select an Nmap Remediation configured earlier. The Nmap Instance is inherently tied to the Nmap Remediation.
 - g. Nmap Target: Select the appropriate Nmap Target configured earlier
 - h. Provide a unique Job Name, e.g. **Nmap-Austin-DMZ** and click *Save*
 - i. Add a new scheduled task for each Nmap instance or target created.

The screenshot shows the 'New Task' configuration interface in the Cisco Firepower Management Center (FMC). The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and System (highlighted in red). Below this is a secondary bar with links for Users, Domains, Integration, Updates, Licenses, Health, Monitoring, and Tools > Scheduling (highlighted in red). The main form is titled 'New Task' and contains the following fields:

- Job Type:** A dropdown menu set to 'Nmap Scan'.
- Schedule task to run:** Radio buttons for 'Once' and 'Recurring' (selected).
- Start On:** Date and time pickers set to August 20, 2016, at America/Chicago.
- Repeat Every:** A text input set to '1', with frequency options for Hours, Days (selected), Weeks, and Months.
- Run At:** Time and AM/PM pickers set to 5:00 PM.
- Job Name:** A text input set to 'Nmap-Austin-DMZ'.
- Nmap Remediation:** A dropdown menu set to 'Nmap-Remed-Austin'.
- Nmap Target:** A dropdown menu set to 'Austin-DMZ'.
- Comment:** A large text area for additional notes.
- Email Status To:** A text field with a message: 'Not available. You must set up your mail relay host.'

At the bottom of the form are 'Save' and 'Cancel' buttons.

Tip: It is important to periodically verify that scheduled Nmap scans are completing successfully. One method is for FMC to email the scan status to an individual or group email address. This is configured in the “Email Status To” section of the scheduled task. Alternatively, assign someone to regularly log in to the FMC and navigate to *Policies > Actions > Scanners*, then *Scan Results*. Clicking on *View* under the Results column will validate that the scheduled scan ran successfully.

2.2.3. Enable automated scanning of new hosts

As new IP addresses appear on the network, Firepower Correlation Policies can trigger Nmap to perform an active scan of the new hosts. As a result, more accurate host profiles are created soon after new systems connect to the network. This is especially helpful for systems that may not be online when scheduled Nmap scans launch.

- ix. Create a correlation rule for detecting new IP hosts
 - a. Navigate to *Policies > Correlation*, then click *Rule Management*
 - b. Click *Create Rule*
 - c. Provide a name for the rule, e.g. **Nmap-NewIP-Austin**
 - d. Provide a rule description and group if desired
 - e. Under *Select the type of event for this rule*, select *a discovery event occurs*
 - f. When the option appears, select *a new IP host is detected*
 - g. In the conditions dropdown, select *IP Address*, then *is in*
 - h. Specify a subnet where automated Nmap scanning is desired when new IP addresses appear.
 - i. Click the *Add condition* button to add additional subnets, then click *Save*

Rule Information

Rule Name: Nmap-NewIP-Austin

Rule Description:

Rule Group: Ungrouped

Select the type of event for this rule

If a discovery event occurs a new IP host is detected and it meets the following conditions:

OR

- IP Address is in 192.168.0.0/16
- IP Address is in 10.10.234.0/24

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".

Save Cancel

Tip: For more accurate and up-to-date host profiles on end-user subnets, extend DHCP lease times to allow hosts to keep their dynamically assigned IP addresses longer, if the environment allows for it. For large, stable networks with plenty of IP space, Microsoft recommends setting a DHCP lease time of 2-3 weeks. Reference:



[https://technet.microsoft.com/en-us/library/cc780311\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc780311(v=ws.10).aspx)

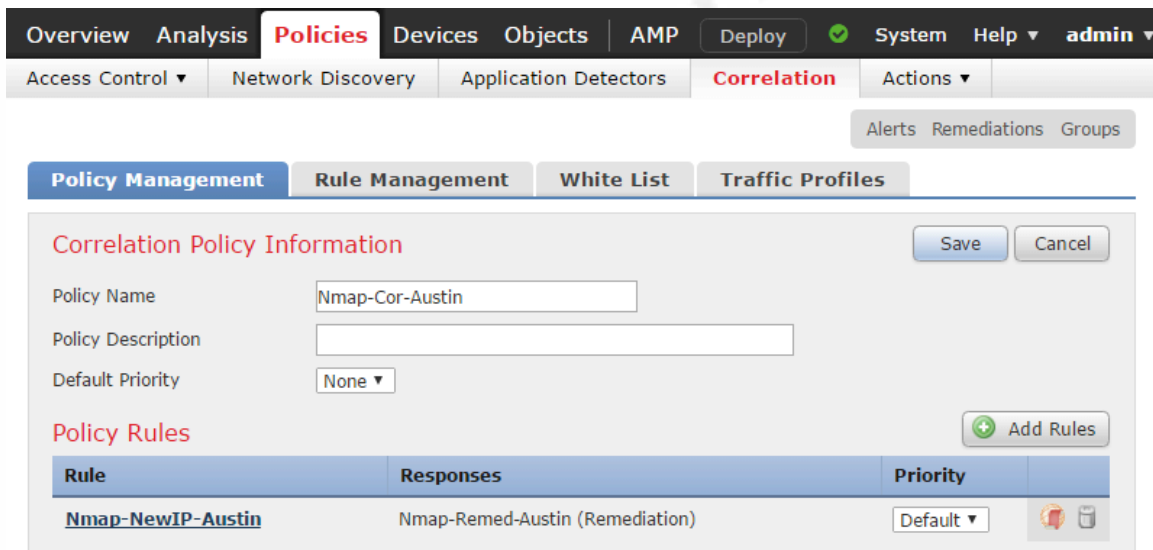
x. Create a Correlation Policy to trigger scanning

The Correlation Policy ties together the Correlation Rule in the previous step to an Nmap Remediation policy. As new IP addresses are seen by Firepower as defined by the Correlation Rule, the selected Nmap Remediation policy is triggered.

a. Navigate to *Policies > Correlation*, then click *Policy Management*

Author Name, email@addressgmail.com

- b. Click *Create Policy*
- c. Provide a policy name, e.g. **Nmap-Cor-Austin**
- d. Click *Add Rules*
- e. Select the correlation rule created in section ix above and click *add*
- f. Click the Responses icon—
- g. Move the desired Nmap Remediation under *Unassigned Responses* into the *Assigned Responses* field and click *Update*
- h. Click Save
- i. Activate the Correlation Policy by moving the slider—



Correlation Policy Information

Policy Name:

Policy Description:

Default Priority:

Policy Rules

Rule	Responses	Priority
Nmap-NewIP-Austin	Nmap-Remed-Austin (Remediation)	Default

Tip: For Firepower to obtain the most accurate information about hosts in the environment, import credentialed scan data from a third-party vulnerability scanner such as Nessus, Nexpose, or Qualys. Through the use of valid host credentials, vulnerability scanners can collect more information about hosts than Nmap, which was not designed to perform authenticated vulnerability scans. See the “Third-Party Product Mappings” section of the Firepower Configuration Guide for details.

2.2.4. Viewing discovery information

Reviewing the Discovery Events table, located under *Analysis > Hosts > Discovery Events*, is a useful way to tell what information FMC is gathering about hosts on the network.

Discovery Events
[Table View of Events](#) > [Hosts](#)

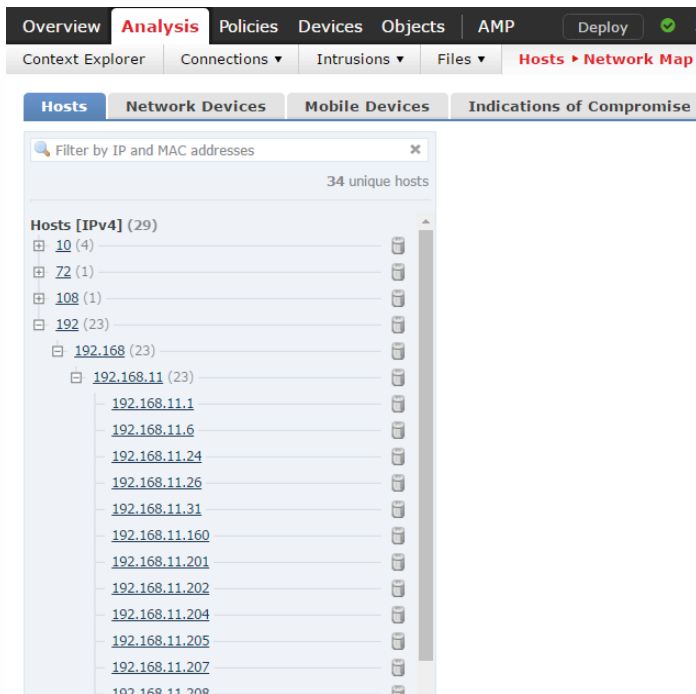
2016-08-29 15:05:00 - 2016-09-05 20:53:47
 Expanding
 Disabled Columns
[MAC Address](#)

▼ Search Constraints ([Edit Search](#) [Save Search](#))
 Event
 VLAN

Jump to...

	Time	Event	IP Address	User	MAC Vendor	Port	Description
↓	2016-09-05 19:36:09	Client Update	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Android browser 5.2/6.0.1 3.C. Pennev
↓	2016-09-05 19:36:09	New Client	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Android browser 5.2/6.0.1
↓	2016-09-05 19:06:25	Client Update	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Pandora 7.5 Pandora Audio
↓	2016-09-05 18:31:33	Client Update	192.168.11.204		Murata Manufacturing Co., Ltd.		HTTPS SSL client Foursquare
↓	2016-09-05 17:22:32	Client Update	192.168.11.204		Murata Manufacturing Co., Ltd.		HTTPS SSL client Atlas Advertiser Suite
↓	2016-09-05 17:10:40	DHCP: IP Address Changed	192.168.11.229		VMware, Inc.		Merged Hosts
↓	2016-09-05 17:10:40	MAC Information Change	192.168.11.229		VMware, Inc.		MAC: 00:0C:29:F0:0B:61 TTL 64 (ARP/DHCP detected)
↓	2016-09-05 17:09:42	Client Update	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Pandora 7.5 Ando Media
↓	2016-09-05 17:05:22	Client Update	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Pandora 7.5 Pandora
↓	2016-09-05 17:05:22	Client Update	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Pandora 7.5 Pandora Audio
↓	2016-09-05 17:03:40	Client Update	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Pandora 7.5 Ando Media
↓	2016-09-05 17:03:40	New Client	192.168.11.216		Murata Manufacturing Co., Ltd.		HTTP Pandora 7.5
↓	2016-09-05 17:02:09	Client Update	192.168.11.204		Murata Manufacturing Co., Ltd.		SSL SSL client Samsung
↓	2016-09-05 16:58:08	Client Update	192.168.11.204		Murata Manufacturing Co., Ltd.		HTTPS SSL client MS CDN

The Network Map under *Analysis > Hosts > Network Map* lists all IP addresses discovered through previously defined discovery policies. Unfamiliar IP addresses may appear in this table, such as IP addresses from subnets that shouldn't exist in the environment. This is normal behavior since hosts will sometimes try to use previously assigned addresses and disconnected VPN adapters for network access.




Analysis > Hosts > Hosts > Table View of Hosts provides a more detailed table of hosts discovered on the network. For certain situations, exporting the data using the FMC Report Designer and analyzing the data using Excel can be incredibly useful.

Overview Analysis Policies Devices Objects AMP										
Context Explorer		Connections ▾		Intrusions ▾		Files ▾		Hosts ▸ Hosts		Users ▾
								Vulnerabilities ▾		Correlation ▾
								Custom ▾		Search

Operating System Summary (switch workflow)
[Summary of OS Names](#) > [Summary of OS Versions](#) > [OS Details with IP, NetBIOS, Criticality](#) > **[Table View of Hosts](#)** > [Hosts](#)
 ▼ Search Constraints [\(Edit Search\)](#)

Jump to... ▾										
▢	▾ Last Seen ×	IP Address ×	MAC Vendor ×	Current User ×	Host Criticality ×	VLAN ID ×	Hops ×	Host Type ×	OS Vendor ×	
⬇	2016-09-05 19:04:36	192.168.11.216	Murata Manufacturing Co., Ltd.		None	11	0	Host	CentOS, Google, Ubuntu	
⬇	2016-09-05 18:44:59	192.168.11.24			None	11	0	Host	CentOS, Google, Ubuntu	
⬇	2016-09-05 18:42:48	192.168.11.204			None		1	Host	CentOS, Google, Ubuntu	
⬇	2016-09-05 18:40:40	192.168.11.229	VMware, Inc.		None	11	0	Host	CentOS, Google, Ubuntu	
⬇	2016-09-05 18:38:52	192.168.11.26	VMware, Inc.		None	11	0	Host	Linux	
⬇	2016-09-05 18:37:26	192.168.11.211			None		0	Host	CentOS, Google, Ubuntu	
⬇	2016-09-05 18:37:25		Cisco Systems, Inc.		None	500	0	Host	pending	
⬇	2016-09-05 18:37:25	192.168.11.202	Intel Corporate	Discovered Identities\anonymous (FTP)	None	11	0	Host	FreeBSD	
⬇	2016-09-05 18:37:23	192.168.11.201	Cisco Systems, Inc.		None	11	0	Host	unknown	

Drill into a host profile to see details about a particular host, either by clicking on the host icon  or navigating to *Analysis > Hosts > Hosts > Hosts*. Further drill-down into operating system and listening services (*Servers*) information is also available.

Host Profile

Scan Host

Generate White List Profile

IP Addresses

192.168.11.219

NetBIOS Name

Device (Hops)

5508 (0)

MAC Addresses (TTL)

00:15:17:BA:B0:8D (Intel Corporate) (255)

Host Type

Host

Last Seen

2016-09-05 22:37:16

Current User

View

[Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (0)

Edit Rule States





































Operating System ▼

Edit Operating System

View Operating Systems

Vendor	Product	Version	Source
Microsoft, Corp.	Windows Vista		Scanner: Nmap

Servers (9) ▼

	Protocol	Port	Application Protocol	Vendor and Version	
	tcp	443	HTTPS		   
!	tcp	5001	complex-link		   
!	tcp	2869	HTTP	Microsoft HTTPAPI httpd 2.0	   
!	tcp	903	vmware-auth	VMware Authentication Daemon 1.10	   
	tcp	135	DCE/RPC	Microsoft Windows RPC	   
	tcp	139	NetBIOS-ssn (SMB)		   
!	tcp	5357	HTTP	Microsoft HTTPAPI httpd 2.0	   
!	tcp	445	NetBIOS-ssn (SMB)		   
!	tcp	4242	vrml-multi-use		   

Applications (122) ▶

Users (no user history available)

Attributes ▼

Edit Attributes

Host Criticality

None

Analysis > Hosts > Hosts > Table View of Applications allows visibility into which applications are running on which hosts.

Application	IP Address	Type	Category
Ad Advisor	192.168.11.208	Web Application	ad portal, business, web services provider
Ad Advisor	192.168.11.216	Web Application	ad portal, business, web services provider
Ad Nexus	192.168.11.216	Web Application	ad portal, business, web services provider
Ad Nexus	192.168.11.208	Web Application	ad portal, business, web services provider
Adap.tv	192.168.11.208	Web Application	web services provider
Adap.tv	192.168.11.216	Web Application	web services provider
Adblade	192.168.11.208	Web Application	ad portal, business, web services provider
Adblade	192.168.11.216	Web Application	ad portal, business, web services provider
Adconion Media Group	192.168.11.208	Application Protocol, Web Application	ad portal, business, social networking, web services provider
Adconion Media Group	192.168.11.216	Application Protocol, Web Application	ad portal, business, social networking, web services provider
Adaptive	192.168.11.216	Web Application	web services provider

Analysis > Hosts > Hosts > Servers show which listening services have been discovered. This report is useful for noticing unwanted services at a glance.

Application Protocol	Vendor	Version	Count
pending			17
NetBIOS-ssn (SMB)			5
HTTP	Microsoft HTTPAPI httpd	2.0	5
HTTPS			4
vml-multi-use			2
vmware-auth	VMware Authentication Daemon	1.10	2
http-proxy			2
HTTP	Cisco IOS http config		2
HTTP			2
FTP			2
DCE/RPC	Microsoft Windows RPC		2
vmware-auth	VMware Authentication Daemon	1.0	1

Author Name, email@addressgmail.com

Drilling into *Table View of Servers* allows for a more detailed look at which listening services are running on which hosts, as well as information such as application risk and estimated business relevance.

Overview **Analysis** Policies Devices Objects AMP

Context Explorer Connections Intrusions Files **Hosts > Servers** Users Vulnerabilities Correlation Custom Search

Bookmark T

Server Details [\(switch workflow\)](#)

[Servers with Vendor](#) > [Servers with Vendor and Version](#) > **Table View of Servers** > Hosts

▼ Search Constraints [\(Edit Search\)](#)

Jump to...	Last Used	IP Address	Port	Protocol	Application Protocol	Vendor	Version	Web Application	Application Risk	Business Relevance	Hits
2016-09-05 18:35:00	192.168.11.1	0/udp	udp	ICMP					Medium	Medium	6521
2016-09-05 17:32:09	192.168.11.1	67 (bootps)/udp	udp	DHCP					Very Low	High	200
2016-09-05 15:50:17	192.168.11.228	5060/tcp	tcp	SIP					Low	Medium	0
2016-09-04 18:54:20	192.168.11.202	21 (ftp)/tcp	tcp	FTP				FTP	Medium	Medium	1
2016-09-04 01:41:26	192.168.11.6	80 (http)/tcp	tcp	HTTP		Cisco IOS http config		Web Browsing	Very Low	Medium	0
2016-09-04 01:41:26	192.168.11.6	23 (telnet)/tcp	tcp	Telnet		Cisco router telnetd			Low	Medium	0
2016-09-04 01:41:26	192.168.11.6	22 (ssh)/tcp	tcp	SSH		Cisco SSH	1.25		High	Medium	0
2016-09-04 01:41:26	192.168.11.6	443 (https)/tcp	tcp	HTTP		Cisco IOS http config		Web Browsing	Very Low	Medium	0
2016-09-04 01:03:27	192.168.11.202	8080/tcp	tcp	http-proxy					Very Low	Very Low	0
2016-09-04 00:39:25	192.168.11.208	902/tcp	tcp	vmware-auth		VMware Authentication Daemon	1.10		Very Low	Very Low	0

2.3. Monitoring device and application compliance

After a high-profile data breach, the board of directors, executives and management are highly motivated to take action and enhance the security posture of the organization. Security budgets increase, additional information security personnel are added, and the culture of the business becomes more accepting of the inconveniences of certain security controls. Unsurprisingly, this motivation is fleeting.

Competing business demands over time may nudge IT professionals to deprioritize addressing security issues, and processes requiring manual action are typically the first to drop off. Because of this, automation is one of the “five critical tenets” of the Critical Security Controls.

For many organizations, an incident management system such as a help desk system is the primary method of ensuring issues are properly tracked and addressed. Automatically creating incident tickets via Firepower email alerts is a common way to automate the process of addressing compliance violations. Syslog or SNMP alerts can also be used to automate the process.

Implementation at-a-glance:	<ol style="list-style-type: none"> 1. Enable compliance violation alerts <ol style="list-style-type: none"> i. Enable email notifications for automated incident/ticket creation 2. Create a Compliance White List with violation alerting <ol style="list-style-type: none"> ii. Create a new White List iii. Create a correlation policy for alerting on White List violations 3. Create Compliance Black Lists using Correlation Policies <ol style="list-style-type: none"> iv. Create a correlation rule defining OS black lists v. Create a correlation rule defining black lists for listening services
-----------------------------	---

	vi. Create a correlation policy for alerting on black list violations
--	---

2.3.1. Enable compliance violation alerts

- i. Enable email notifications for automated incident/ticket creation
 - a. Navigate to *System > Configuration*, then click *Email Notification*
 - b. Configure Mail Relay information according to your organization's requirements
 - c. Click the *Test Mail Server Settings* button, then if successful, click *Save*

- d. Under *Polices > Correlation* click on *Alerts* in the top-right menu
- e. Select *Create Alert > Create Email Alert*
- f. Provide a name, e.g. **FMC Compliance Violation**
- g. Under *To*, provide an email address where compliance violation alerts will be sent. Starting out, specify your personal email address or a test account. After necessary tweaking/tuning has been performed to reduce alerting noise, specify an email address that will automatically open incident tickets.

- h. In the *From* field, specify which email address will appear as the sender. This does not necessarily need to be a legitimate address.
- i. Click *Save*, then ensure the rule is enabled by adjusting the slider, if necessary

Edit Email Alert Configuration

Name: FMC Compliance Violation

To: RyanQFirth+gccc@gmail.com

From: FMC@example.com

Relay Host: smtp-mail.outlook.com

Alert Configuration is in use by 2 Policies.

Save Cancel

2.3.2. Create a Compliance White List with violation alerting

Compliance white lists are used to specify the operating systems, applications, or protocols permitted on target networks. Three types of white list profiles exist—global, operating-system specific, and shared.

A “Global” profile is operating-system agnostic. For example, the FTP protocol can be added to a global white list, thereby approving it to run on any operating system in the target networks.

If FTP is only approved to run on Windows operating systems, it can be listed in a Windows “Operating-system specific” profile, which is used by a single white list. Shared profiles allow operating-system criteria to be used across multiple white lists. For more details, see the Firepower Management Center Configuration Guide under “Compliance White Lists.”

- ii. Create a new White List

In this example, the target network is a DMZ containing Windows, Linux, and Cisco systems, residing on subnet 192.168.11.0/24. Web services on ports 80 and 443 are permitted on all operating systems within the DMZ. Host and application discovery (as

configured in the prior section) has been running on this network for the last week to aid in white list auto-creation.

- a. Navigate to *Policies > Correlation > White List* and click *New White List*
- b. Add a target IP address of 192.168.11.0 with a netmask of 24
- c. Click *Add and Survey Network*.

Note: By selecting “Survey Network” FMC will use discovery data to automatically create host profiles. This can dramatically speed-up the process of creating White Lists, and is highly recommended. Under *Allowed Host Profiles*, all operating systems previously detected to exist within the target network are listed.



- d. Provide a unique name for the White List, e.g. **Austin DMZ**
- e. Add a shared host profile to be used against all Linux systems across all white lists.
 - i. Click *Add Shared Host Profile*
 - ii. Select *Linux 2.4 and 2.6 Based Systems* then click *OK*. The host profile appears under *Allowed Host Profiles* in italics to indicate that it is a shared host profile.
 - iii. (Optional) Click *Edit* to change any settings in the shared host profile. Changing shared host profiles will affect all White Lists where the shared profile exists.
- f. (Optional) Click on a host profile to edit Allowed Application Protocols, Allowed Clients, Allowed Web Applications, or Allowed Protocols. Tweaking the OS Vendor or Name fields may also be desired.
- g. (Optional) Click the trashcan icon next to operating systems that are not allowed on the target network. Operating systems not specifically listed will be in violation of the White List.
- h. Allow any host in the target network to run services listening on TCP ports 80 and 443.
 - i. Click *Any Operating Systems*

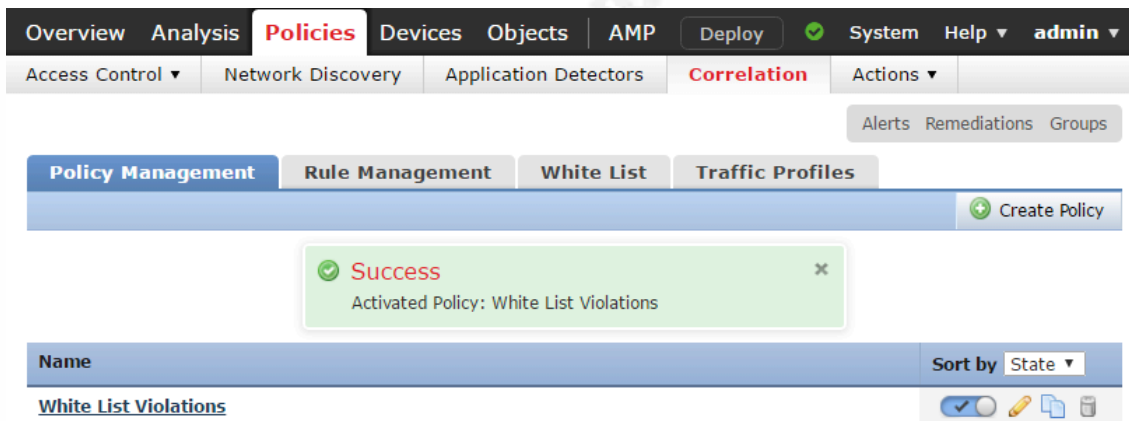
- ii. Click the plus symbol next to *Globally Allowed Application Protocols*
- iii. Use the Ctrl key to select both *HTTP/80 TCP* and *HTTPS/443 TCP* then click *OK*

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, Deploy, System, Help, and admin. Below this is a sub-navigation bar with Access Control, Network Discovery, Application Detectors, Correlation (selected), and Actions. The main content area is divided into Policy Management, Rule Management, White List (selected), and Traffic Profiles. Under White List, there are buttons for Add Shared Host Profile and Target Network. The left pane shows a tree view for the 'Austin DMZ' policy, with 'Target Networks' containing '192.168.11.0/24' and 'Allowed Host Profiles' containing 'Any Operating System'. The right pane shows the configuration for 'Any Operating System', with sections for Globally Allowed Application Protocols (containing 'HTTP/80 TCP' and 'HTTPS/443 TCP'), Globally Allowed Clients, Globally Allowed Web Applications, and Globally Allowed Protocols. At the bottom, there are 'Save White List' and 'Cancel' buttons.

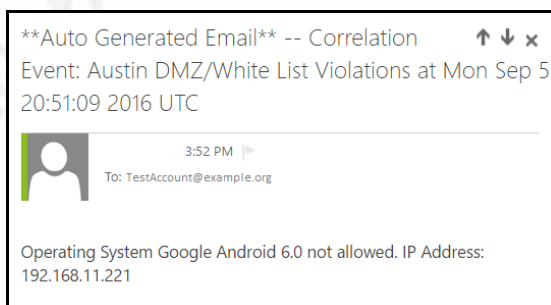
- i. Click *Save White List*

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, Deploy, System, Help, and admin. Below this is a sub-navigation bar with Access Control, Network Discovery, Application Detectors, Correlation (selected), and Actions. The main content area is divided into Policy Management, Rule Management, White List (selected), and Traffic Profiles. Under White List, there are buttons for Edit Shared Profiles and New White List. A green success message box is displayed, stating 'Success Saved White List: Austin DMZ'. Below this, a table lists the white lists: 'Austin DMZ' and 'Default White List' (Recommended White List). Each entry has edit, copy, and delete icons.

- iii. Create a correlation policy for alerting on White List violations
 - a. Navigate to *Policies > Correlation > Policy Management*
 - b. Click Create Policy
 - c. Provide a policy name, e.g. **White List Violations**
 - d. Click *Add Rules*
 - e. Select the white list created in the previous section and click *Add*
 - f. Click the “Responses” icon next to a rule. 
 - g. Move the “FMC Compliance Violation” response created earlier in this section into the *Assigned Responses* box and click *Update*
 - h. Repeat this process for any other White Lists, then click *Save*
 - i. Enable the rule by sliding the “Activate” button 



An example of a white list policy violation email:



Author Name, email@addressgmail.com

Note: FMC does not create new white list events for existing violations. Only new violations will trigger a white list event.

View White List events by navigating to *Analysis > Correlation > White List Events*

White List Events
[Table View of White List Events](#)
 Search Constraints ([Edit Search](#))

2016-08-29 15:05:00 - 2016-09-05 23:13:05
 Expanding
 Disabled Columns
[Port](#)
[User](#)

Time	IP Address	Description	Policy	White List
2016-09-05 15:51:09	192.168.11.221	Operating System Google Android 6.0 not allowed. IP Address: 192.168.11.221	White List Violations	Austin DMZ
2016-09-05 15:49:58	192.168.11.228	Operating System Google Android 6.0 not allowed. IP Address: 192.168.11.228	White List Violations	Austin DMZ
2016-09-05 15:48:04	192.168.11.229	Operating System CentOS Linux 6.3, 6.4 not allowed. IP Address: 192.168.11.229	White List Violations	Austin DMZ

Violations to White Lists can be seen by navigating to *Analysis > Correlation > White List Violations*. Sorting violation counts in descending order provides a quick way to find which systems deviate the most from the defined standard.

Host Violation Count ([switch workflow](#))
[Host Violation Count](#) > [Table View of White List Violations](#) > [Hosts](#)
 No Search Constraints ([Edit Search](#))

IP Address	White List	Count
192.168.11.216	Austin DMZ	202
192.168.11.208	Austin DMZ	144
192.168.11.202	Austin DMZ	106
192.168.11.204	Austin DMZ	54
192.168.11.219	Austin DMZ	40
192.168.11.217	Austin DMZ	27
192.168.11.221	Austin DMZ	22
192.168.11.207	Austin DMZ	22
192.168.11.228	Austin DMZ	21
192.168.11.213	Austin DMZ	10

Author Name, email@addressgmail.com

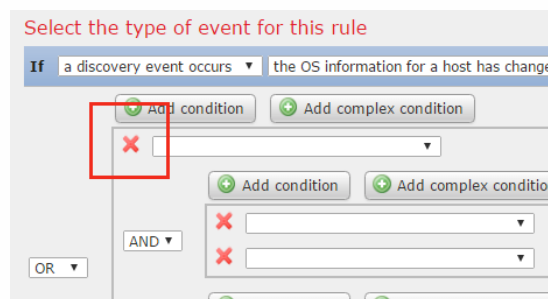
2.3.3. Create Compliance Black Lists using Correlation Policies

In some environments, defining which operating systems and listening services should *not* exist within a network (black lists) may be preferred over trying to define what all should exist (white lists). While black lists in this manner do not exist as a defined feature within Firepower, tying together Discovery Events with Correlation Rules can allow for the effective creation of black lists.

- iv. Create a correlation rule defining OS black lists

In this example, Linux, Ubuntu, and Apple operating systems are not permitted on subnets 192.168.11.0/24 and 10.180.234.0/24.

- a. Navigate to *Policies > Correlation > Rule Management*, then click *Create Rule*
- b. Provide a rule name, e.g. **Banned OSs-Linux, Apple** and a description, if desired
- c. (Optional) For better organization, create then select a Rule Group, e.g. **Banned Oss, Services-Group**
- d. Under “Select the type of event...” use the drop-down to select *a discovery event occurs*
- e. A new drop-down will appear. Select *the OS information for a host has changed*
- f. Click *Add complex condition*, then again after the page reloads
- g. Delete the top condition



- h. For the new top condition, use the drop-down to select *OS Vendor*

- i. When the new drop-down menus appear, select *is Linux or Ubuntu*
- j. Repeat the process to select *Apple*
- k. Change the closest operator from *AND* to *OR*. This configures FMC to look for either Linux or Ubuntu, or Apple.
- l. In the second set of complex conditions, use the drop-down to select *IP Address*
- m. When the new drop-down menus appear, select *is in* then specify a subnet where Linux, Ubuntu, or Apple should not exist. e.g. **192.168.11.0/24**
- n. Repeat the process for any additional subnets this rule should apply. Click *Add condition* to add more than two subnets.
- o. Change the closest operator from *AND* to *OR*.
- p. (Optional) To add exceptions to this correlation rule, add a third set of complex conditions. Select *IP Address, is not*, then the IP address of the exception.
- q. Change the outer operator from *OR* to *AND*, then click *Save*

Policy Management | **Rule Management** | White List | Traffic Profiles

Rule Information

Rule Name: Banned OSs-Linux, Apple

Rule Description: Linux or Mac in Windows subnets

Rule Group: Banned OSs, Services-Group

Select the type of event for this rule

If a discovery event occurs the OS information for a host has changed and it meets the following conditions:

OR

AND

OR

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".

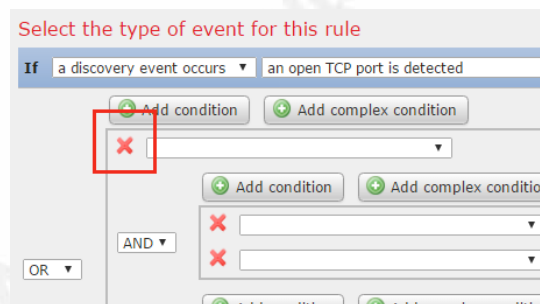
Save Cancel

Caution: Even through the use of Nmap discovery, in some situations, FMC may frequently assign incorrect operating systems to a host. Because IPS rules are enabled based on which operating systems exist, FMC may add an operating system to a host profile even if there's a good chance that assignment is incorrect. (Erring on the side of caution for the benefit of IPS coverage) Due to this behavior, the use of correlation rules to create operating system black lists may generate too many false positives to be useful on some networks. Utilizing compliance white lists, as specified earlier, may provide an alternative. Where OS detection and system profiling are critical, Cisco ISE (Identity Services Engine) should be considered.

- v. Create a correlation rule defining black lists for listening services.

In this example, systems on subnets 192.168.11.0/24 and 10.180.234.0/24 are not permitted to run services listening on TCP ports 80, 22, and 21.

- a. Navigate to *Policies > Correlation > Rule Management*, then click *Create Rule*
- b. Provide a rule name, e.g. **Banned Services-CorpUsers**, and a description, if desired
- c. (Optional) For better organization of correlation rules, create, then select a Rule Group, e.g. **Banned OSs, Services-Group**
- d. Under “Select the type of event...” use the drop-down to select *a discovery event occurs*
- e. A new drop-down will appear. Select *an open TCP port is detected*
- f. Click *Add complex condition*, then again after the page reloads
- g. Delete the top condition



- h. For the new top condition, use the drop-down to select *Application Port*
- i. When the new drop-down menus appear, select *is* then type **80**
- j. Repeat the process for port 22
- k. Click the nearest *Add condition* button and repeat the process for port 21
- l. Change the closest operator from *AND* to *OR*. This configures FMC to look for either ports 80, 22, or 21.

- m. In the second set of complex conditions, use the drop-down to select *IP Address*
- n. When the new drop-down menus appear, select *is in* then specify a subnet where hosts should not run services listening on ports 80, 22, or 21. e.g. **192.168.11.0/24**
- o. Repeat the process for any additional subnets this rule should apply. Click *Add condition* to add more than two subnets.
- p. Change the closest operator from *AND* to *OR*.
- q. (Optional) To add exceptions to this correlation rule, add a third set of complex conditions. Select *IP Address, is not*, then the IP address of the exception.
- r. Change the outer operator from *OR* to *AND*, then click *Save*

Policy Management | **Rule Management** | White List | Traffic Profiles

Rule Information

Rule Name: Banned Services-CorpUsers

Rule Description:

Rule Group: Banned OSs, Services-Group

Select the type of event for this rule

If a discovery event occurs an open TCP port is detected and it meets the following conditions:

Add condition Add complex condition

OR

AND

Add condition Add complex condition

Application Port is 80

Application Port is 22

Application Port is 21

OR

IP Address is in 192.168.11.0/24


IP Address is in 10.180.234.0/24

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".

Save Cancel

- vi. Create a correlation policy for alerting on black list violations
 - a. Navigate to *Policies > Correlation > Policy Management*
 - b. Click Create Policy
 - c. Provide a policy name, e.g. **Banned OSs, Services-Policy**
 - d. Click *Add Rules*
 - e. Select the black lists created in the previous section and click *Add*
 - f. Click the “Responses” icon next to a rule. 
 - g. Move the “FMC Compliance Violation” response created earlier in this section into the *Assigned Responses* box and click *Update*

h. Repeat this process for all violation rules, then click *Save*

Correlation Policy Information

Policy Name:

Policy Description:

Default Priority:

Policy Rules

Rule	Responses	Priority
<u>Banned OSs-Linux, Apple</u> Linux or Mac in Windows subnets	FMC Compliance Violation (Email)	Default
<u>Banned Services-CorpUsers</u>	FMC Compliance Violation (Email)	Default

i. Enable the rule by sliding the “Activate” button ☒

Policy Management

Success: Activated Policy: Banned OSs, Services-Policy

Name	Sort by	State
<u>Banned OSs, Services-Policy</u>	State	<input checked="" type="checkbox"/>
<u>Nmap-Cor-Austin</u>		<input checked="" type="checkbox"/>

An example of an email alert generated when a black listed operating system appears:

Auto Generated Email --

Correlation Event: Banned OSs-Linux, Apple/Banned OSs, Services-Policy at Mon Sep 5 20:41:54 2016 UTC

3:44 PM
To: TestAccount@example.org

<*- New OS From "5508" at Mon Sep 5 20:41:53 2016 UTC -
*> IP Address: 192.168.11.204 OS: Google Android Android 6.0 Device Info: mobile last_seen: 1473108113

Author Name, email@addressgmail.com

3. Measuring and testing the controls

3.1. CIS control measurements

Establishing measurements/metrics around security controls is essential for any security program. Organizations attempting to strengthen their security posture can use metrics to gauge progress or identify stalled efforts. If metrics are properly tracked and reported to the business, unacceptable or deteriorating program performance can be addressed proactively. For example, suppose a systems engineering team isn't staffed appropriately to comply with a 30-day patch window for the servers they maintain. Establishing agreed-upon metrics from all stakeholders involved, then regularly reporting on those metrics to the appropriate stakeholders will keep the risks top of mind. Perhaps the business isn't able to add headcount or adjust the priority of patching. In that case, the business may have to accept the risk of a 60-day patch window and adjust the security control accordingly. In any case, solid, thoughtful measurements of security controls help keep expectations aligned between the security team and the rest of the organization.

In *A Measurement Companion to the CIS Critical Security Controls (Version 6)*, several “Measures, Metrics, and Thresholds” are recommended for each Critical Control. Those relevant for measuring the items outlined in this paper are as follows. Security teams, with guidance from their organization, are encouraged to create and track additional metrics most relevant to their security program.

3.1.1. CIS measurement 1.1

“How many unauthorized devices are presently on the organization's network (by business unit)?”

Example Implementation

1. Select a group of subnets for testing that all fall within similar management oversight if possible, such as the corporate desktop subnets, or all Internet DMZ subnets. As metrics are tracked and reported over time, allowing a manager the greatest ability to improve those metrics through full ownership will typically produce the best results.
2. Export an inventory list from the corporate asset management system in csv format

Author Name, email@addressgmail.com

- a) To adhere to CSC 1.4, all systems with an IP address on the network should have the following items recorded in the asset inventory: “network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device.” (CIS, 2015)
3. Generate an export of the host data table in Firepower
 - a) Navigate to *Analysis > Hosts > Hosts > Table View of Hosts*
 - b) Click *Edit Search*
 - c) Enter the relevant subnets in the *IP Address* cell, comma-separated, then click *Search*
 - d) Click on the *Report Designer* link
 - e) In the *Report Sections* area, keep only the *Table View of Hosts* section, which should contain the following settings:
 - i) *Table = Hosts*
 - ii) *Preset = None*
 - iii) *Format = Table View*
 - iv) *Search = Event Viewer*
 - v) *All other settings default*
4. Click *Generate*. For the *Output Format*, select CSV and click *Generate* then *Yes*
5. Open the CSV file contained in the zip download. This file should contain all hosts known by Firepower that exist within the selected subnets.
6. Combine both CSV files into a single Excel workbook.
7. Compare the asset inventory output with the Firepower host report.

- a) Use unique attributes to compare the data in the two spreadsheets using Excel's VLOOKUP or INDEX & MATCH functions. See <https://support.office.com/en-us/article/Look-up-values-with-VLOOKUP-INDEX-or-MATCH-7144ef3f-e322-4f95-9e96-f1d743270438> for details.
8. The reported metric will be either a sum or percentage of all hosts reported by Firepower that do not exist in the asset inventory for the target subnet.
9. Scheduled reports combined with a business intelligence tool such as Microsoft Power BI or Tableau can help automate this process.

3.1.2. CIS measurements 1.2 & 2.6

1.2 – “How long, on average, does it take to remove unauthorized devices from the organization's network (by business unit)?”

2.6 – “How long does it take to remove unauthorized software from one of the organization's systems (time in minutes - by business unit)?”

Example Implementation

The prerequisites to these measurements are first knowing, A) what is an unauthorized device or unauthorized software, B) what time an unauthorized device or software connected to the network, and C) what time the device or software was removed.

Implementing White List and Black List automation as described earlier in this document in addition to automating CIS Measurement 1.1 will assist with A and B. The closure of the incident ticket or utilizing another “time” field within the incident ticket can serve as the official time of device removal. Once all prerequisites have been established, calculating the average time it takes to close compliance violation tickets can serve as the metric.

3.2. Effectiveness tests

An audit or evaluation team outside the management chain of those implementing security controls should regularly test the controls' effectiveness. Effectiveness testing should not be performed via a checklist of control implementation. Rather, practical tests

focused on the results of performing both common and malicious actions should be utilized. These tests should align with the threats addressed by each control.

In *A Measurement Companion to the CIS Critical Security Controls* (Version 6), several “Effectiveness Tests” are recommended. These examples from the Measurement Companion are provided to help generate ideas for effectiveness tests unique to your environments. The “Effectiveness Test for CSC 1 (Inventory of Authorized and Unauthorized Devices)” states:

To evaluate the implementation of CSC 1 on a periodic basis, the evaluation team will connect hardened test systems to at least 10 locations on the network, including a selection of subnets associated with demilitarized zones (DMZs), workstations, and servers. Two of the systems must be included in the asset inventory database, while the other systems are not. The evaluation team must then verify that the systems generate an alert or email notice regarding the newly connected systems within 24 hours of the test machines being connected to the network. The evaluation team must verify that the system provides details of the location of all the test machines connected to the network. For those test machines included in the asset inventory, the team must also verify that the system provides information about the asset owner.

The “Effectiveness Test for CSC 2 (Inventory of Authorized and Unauthorized Software)” states:

To evaluate the implementation of CSC 2 on a periodic basis, the evaluation team must move a benign software test program that is not included in the authorized software list to 10 systems on the network. Two of the systems must be included in the asset inventory database, while the other systems do not need to be included. The evaluation team must then verify that the systems generate an alert or email notice regarding the new software within 24 hours. The team must also verify that the alert or email is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team must verify that the system provides details of the location of each machine with this new test software, including information about the asset owner. The evaluation team must

then verify that the software is blocked by attempting to execute it and verifying that the software is not allowed to run. On systems where blocking is not allowed or blocking functionality is not available, the team must verify that the execution of unauthorized software is detected and results in a notification to alert the security team that unauthorized software is being used.

4. Wrapping up and going further

While other security frameworks, such as NIST 800-53, ISO 27000, and COBIT are more comprehensive, they may be too unwieldy for many resource-strapped security programs. The focused, prioritized approach of the Critical Security Controls make it an incredibly effective tool for those in charge of an organization's information security.

This paper focused on addressing some of the sub-controls found in Critical Security Controls 1 & 2. Cisco Firepower can also help to fully comply with the following sub-controls in Critical Security Controls version 6.0: 6.5, 7.5, 7.6, 8.5, 8.6, 9.1, 9.3, 9.4, 11.2, 12.1, 12.3, 12.4, 12.8, 12.10, 13.7, 13.8, 14.1, and 15.2. Additionally, Firepower can partially assist with the implementation of these sub-controls: 3.6, 4.6, 5.9, 6.4, 11.1, 11.3, 11.5, 11.6, 12.2, 13.3, and 14.2.

If a security team lacks either the technical know-how or time to implement these controls, Cisco Advanced Services or a Cisco Partner can provide professional services to assist. To learn more about Firepower, or anything else in the Cisco portfolio, here are a few training resources:

- Cisco Learning Locator – Locate Cisco authorized training classes for either online or in-person training:
<http://learninglocator.cloudapps.cisco.com/GlobalLearningLocator/LLocatorHome.do>
- Cisco Live – Cisco Live events are scheduled throughout the year around the world, and offer a massive catalog of the most up-to-date training sessions directly from Cisco. In addition, the free online archive of past Cisco Live events is incredibly valuable: <https://www.ciscolive.com>

- Cisco Learning Network – The central hub of Cisco training. Access community forums, videos, study groups, certification tracks, and other training/study material: <https://learningnetwork.cisco.com>
- dCloud – Cisco's on-demand demo portal, providing quick access to experience the latest products in the Cisco portfolio. Labs, training, and walk-through documents are available for many of the modules within dCloud.
<https://dcloud.cisco.com> (Free registration required)

References

The CIS Critical Security Controls for Effective Cyber Defense [PDF]. (2015, October 15). Center for Internet Security (CIS).

A Measurement Companion to the CIS Critical Security Controls (Version 6) [PDF]. (2015, October 15). Center for Internet Security (CIS).

Firepower Management Center Configuration Guide, Version 6.0.1 [PDF]. (2016, August 29). Cisco Systems.

Next-Generation Firewalls (NGFWs) - Gartner IT Glossary. Retrieved September 07, 2016, from <http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws/>

Acknowledgements

Sam Camarda, Cisco Security Consulting Systems Engineer, for excellent, timely feedback.

Author Name, email@addressgmail.com

Appendix-A

Quick Reference

2. Implementation of the Controls	6
2.2. Implementing discovery	7
2.2.1. Enable passive inventory discovery	8
2.2.2. Enable scheduled Nmap scanning	11
2.2.3. Enable automated scanning of new hosts	17
2.2.4. Viewing discovery information	20
2.3. Monitoring device and application compliance.....	26
2.3.1. Enable compliance violation alerts	27
2.3.2. Create a Compliance White List with violation alerting	28
2.3.3. Create Compliance Black Lists using Correlation Policies	33
3. Measuring and testing the controls.....	40
3.1. CIS control measurements.....	40
3.2. Effectiveness tests	42