BCNET

Shared IT Services for Higher Education & Research

Conference 2017

Case Study:

Implementation of Sourcefire Next Generation Intrusion Prevention System at Camosun College.

Case Study:

- Implementation of Sourcefire Next Generation Intrusion Prevention System at Camosun College.

About Camosun:

- Camosun College (http://camosun.ca) is a local community college in Victoria, British Columbia with over 19,000 full-time and part-time students.
- It is currently comprised of two main campuses (Lansdowne and Interurban) and six satellite locations.

Camosun network services

- In general the following devices and services utilize the Camosun network:
  - Staff and Faculty Workstations and Laptops
  - Lab systems and laptop carts
  - Web Services (Internet and Intranet)
  - Multifunction printers and scanners
  - On premise and off premise ("cloud") server based technologies (both physical and virtual):
    - E-mail, Authentication, DNS, Storage, Backups, etc…(this is a big list)
  - Audio visual devices (projectors, smart TVs)
  - Telephone Services (VOIP)
  - Physical Security (Camera, Access Control Systems, and Alerting)
  - Building Environmental Controls
  - Wireless / Wi-fi access
    - Public, Student and Staff wireless access (BYOD ~ 3600 associations per day)
  - VPN site to site and client based authentication and access

The challenge

Based on the previous list of devices, end users, and services:

How do we balance security against performance and connectivity?

In particular, how do you set a network policy for BYOD (unmanaged) devices and the “Internet of Things”?

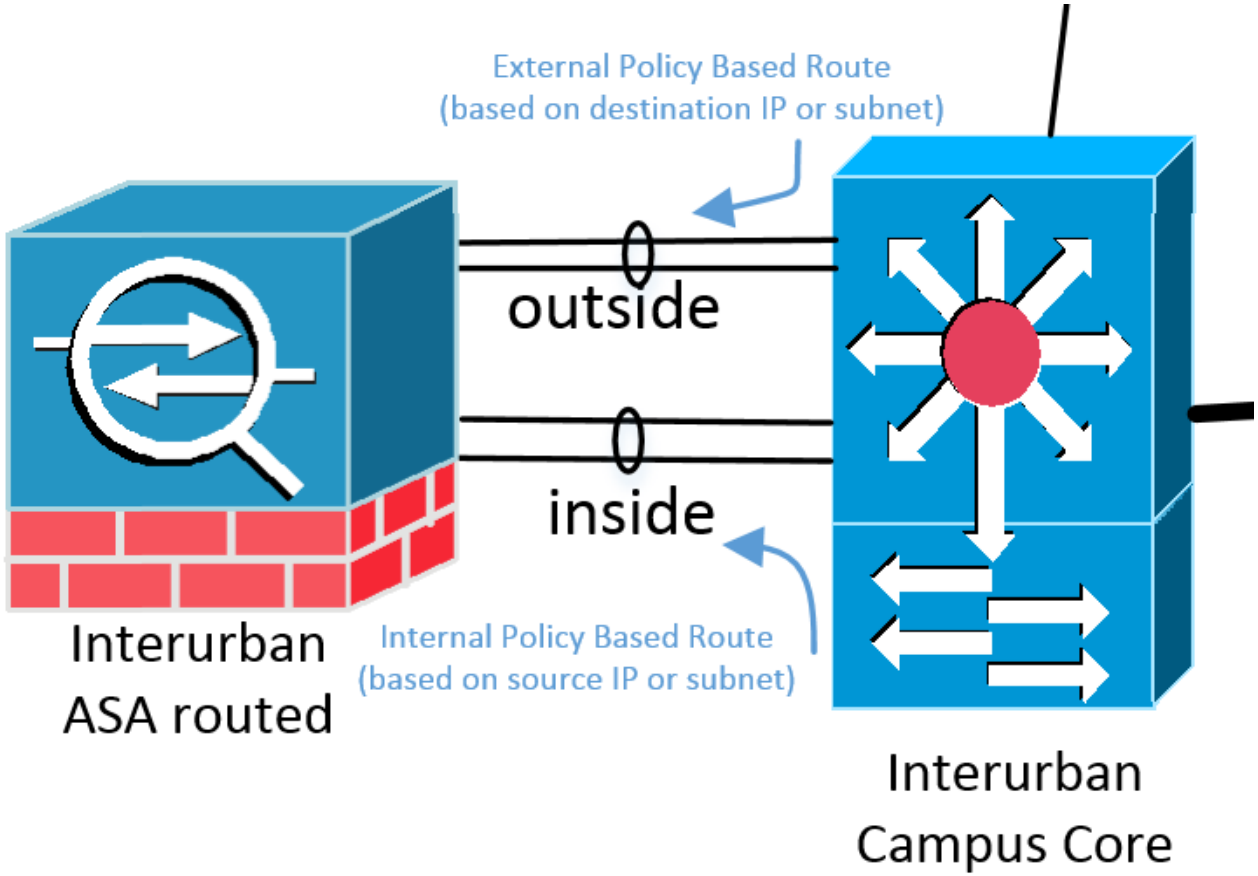
The original solution :

At the Interurban campus in 2014, an existing Cisco ASA 5525-X was configured in routed mode with CX (Context Aware services).

The CX service was configured on a separate software module (much like a line card.). The CX module runs independently of the standard ASA firewall services.

The ASA 5525-X appliances were originally procured in 2012 based on Internet traffic metrics collected via SNMP.

The original CX (Context aware solution)…



Redirecting traffic through the appliance via a policy based route:

- Implementing a policy based route on our Interurban core allowed us to redirect outbound traffic destined to the internet to the internal firewall interface.
- To complete the flow, a matching inbound route policy was applied to redirect traffic from the internet to the external interface.
- This allowed us to test and phase in the appliance by redirecting specific subnets and individual hosts to the new appliance.

Redirecting traffic through the appliance via a policy based route:

- Using the CX service and AVC (Application Visibility and Control) licensing, traffic was monitored. Based on the monitoring results, specific AVC policies were phased in.
- At the time, AVC (Application Visibility and Control) licenses allowed us to curtail undesirable wireless BYOD peer to peer file sharing traffic. For example bit torrent traffic, which previously resulted in numerous copyright infringement notifications direct to the college. The AVC policy significantly reduced issues associated with BYOD peer to peer file sharing.
- However, more recently, NBAR (Network Based Application Recognition) on our new Cisco Wireless Controllers also assists with setting a network application policy for wireless devices.

The Sourcefire acquisition…

- On October 7th, 2013 Cisco completed the acquisition of Sourcefire, Inc.
- Sourcefire, Inc was originally founded by Martin Roesch who is the original creator of the open source network Intrusion Prevention System named - - > “Snort”.

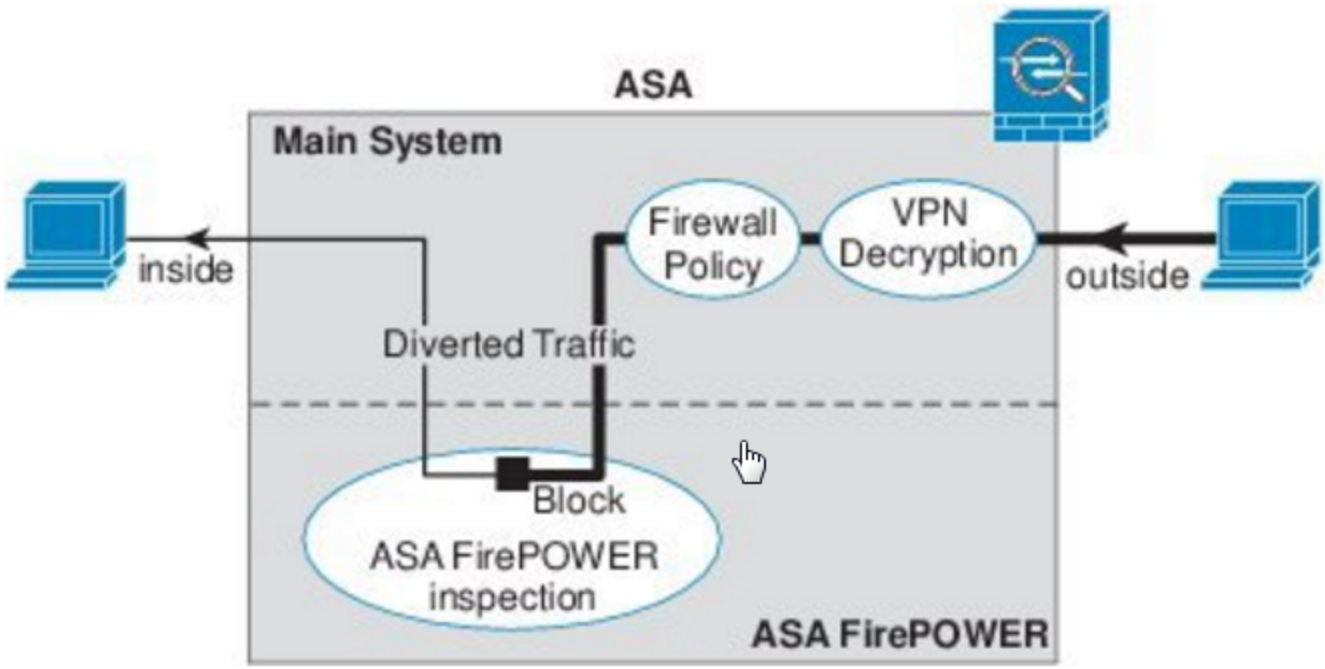
The Sourcefire acquisition…

- The URL for Open Source Snort is https://www.snort.org
- The commercial offering of the Snort software was originally the “Sourcefire 3D” system, which then evolved into the “Firepower” line of security products.
- Roughly, one year after the Sourcefire acquisition, the ASA “Firepower” software module became available for ASA 5500-X appliances.

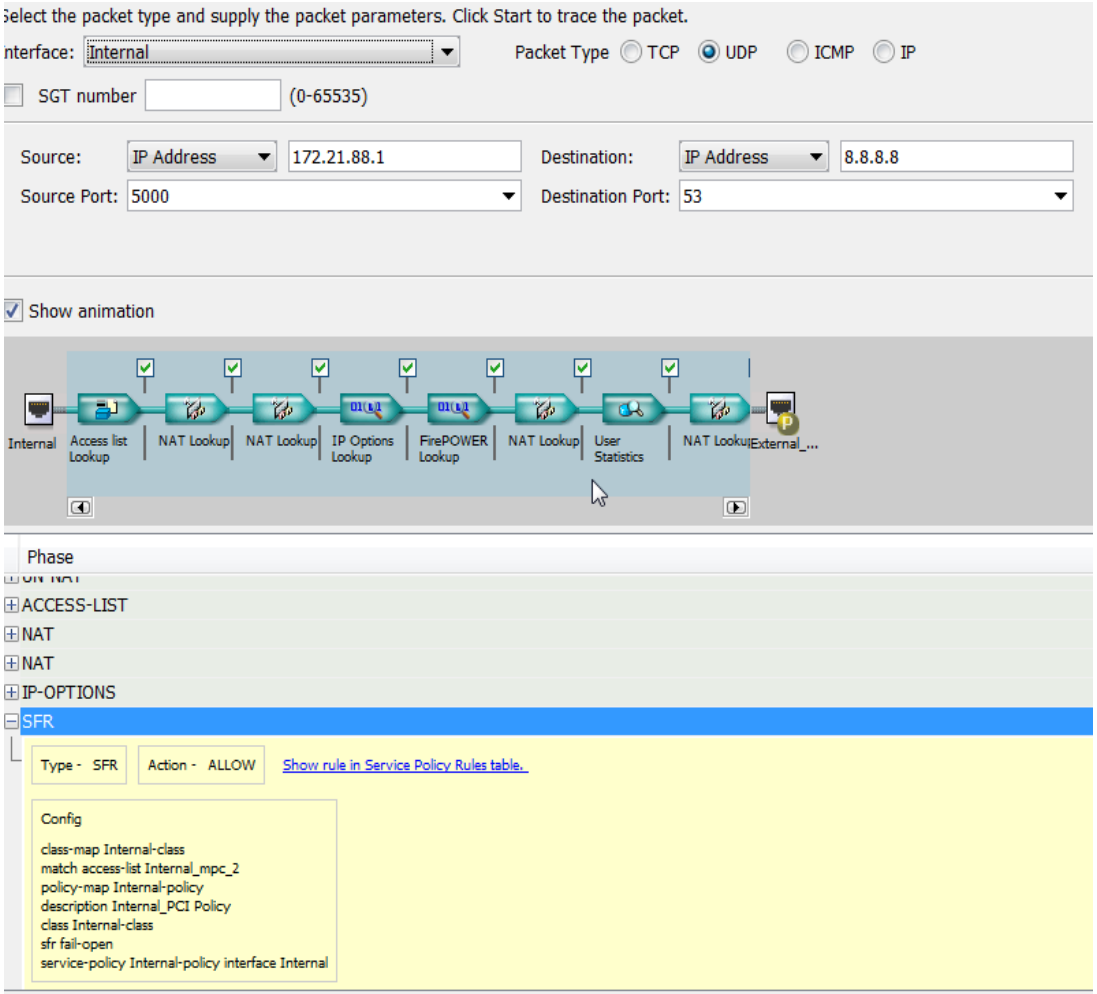
Post Sourcefire Acquisition, the new ASA with FirePOWER module

- The ASA FirePOWER module provides the following next generation firewall services:
  - NGIPS – Next Generation Intrusion Prevention System
  - AVC – Application Visibility and Control
  - URL filtering – URL/Web Reputation Categorization such as Malware, Phishing, Spam, etc…
  - AMP – Advanced Malware Protection (file reputation based on file sha256 hash)

Excerpt from the "Cisco ASA FirePOWER Module Quick Start Guide: FirePower traffic flow in the ASA



FirePOWER lookup as seen by the Packet Tracer:



Camosun - PCI Compliance

- In 2015, as part of a PCI DSS project (Payment Card Industry Data Security Project), Camosun procured the following licensing for the existing ASA 5525-X appliances:
  - Protect and Control (Application Visibility and Control)
  - Firepower IPS
  - AMP – Advanced Malware Protection
  - URL Filtering
- Additionally, a higher capacity ASA 5545-X appliance with the same licensing was procured for the Lansdowne Campus.

Firepower Management Center

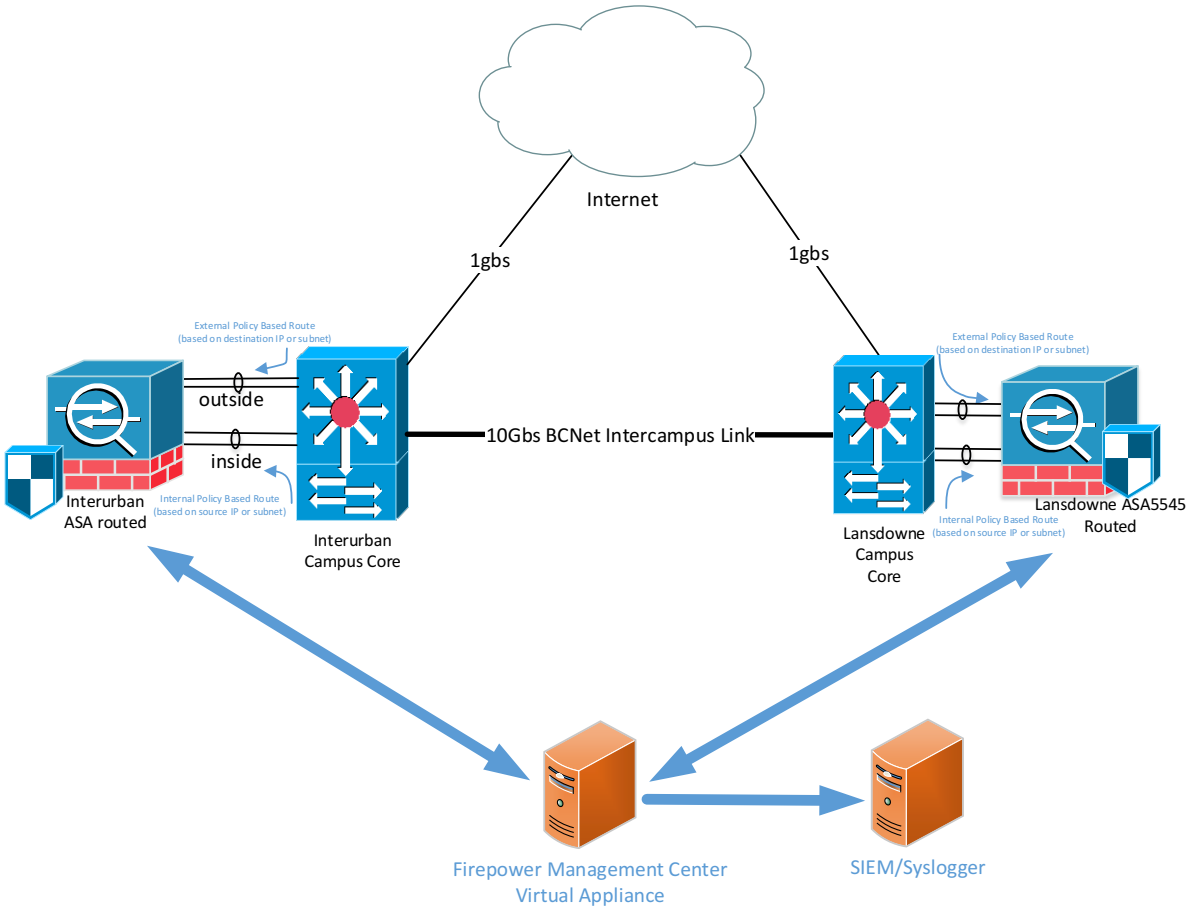
While it is possible to run an ASA with Firepower services as a standalone device. For example, on a smaller 5506-X or 5512-X appliance, it is much more powerful when used in conjunction with Firesight Management Center (historically known as Defence Center).

Therefore, in addition to the Cisco ASA Firepower licensing, Camosun procured licensing for a “FireSIGHT Management Center” virtual appliance (aka Defence Center). Now known as “Cisco Firepower Management Center”.

Firepower Management Center cont…

- The Cisco Firepower Management Center virtual appliance is VERY easy to configure and deploy. It can be downloaded from the Cisco support site as a VMWare .OVA file.
- The virtual management center can manage up to 25 sensors, store up to 10 million events with 250GB of storage
- Additionally, the Virtual appliance can store information on up to 50 thousand network hosts and up to 50 thousand users.

Interurban and Lansdowne Campus Sourcefire configuration



Firepower Management Center.

- The ASA Firepower Management Center centrally configures policy and deploys the desired policy to the ASA with Firepower Services. The ASA's with Firepower services are simply agents which act as inline sensors. These sensors/inline agents carry out and report on events as specified by centrally configured policy.
- *** The real intelligence and functionality is consolidated in the Firepower Management Center ***

Phasing in Sourcefire at Camosun

- Over time, using both policy based routes or ASA service policies Camosun traffic was diverted to the Sourcefire module.
- For each access policy applied to a sensor, there is a default IPS policy (if traffic does not match a defined rule).

Phasing in Sourcefire at Camosun

--System-Provided Policies--

Access Control: Block All Traffic

Access Control: Trust All Traffic

Network Discovery Only

Intrusion Prevention: Maximum Detection

Intrusion Prevention: Connectivity Over Security

Intrusion Prevention: Balanced Security and Connectivity

Intrusion Prevention: Security Over Connectivity

--User Created Policies--

Intrusion Prevention: Initial Inline Policy - Sourcefire3D.intra.camosun.b...

Intrusion Prevention: Wireless_IPS

Intrusion Prevention: Strong_IPS_Policy

Intrusion Prevention: PCI_Web

Intrusion Prevention: Camosun_Staff_IPS

Intrusion Prevention: Initial Passive Policy - Sourcefire3D.intra.camosun...

Phasing in Sourcefire at Camosun and the Change Advisory Board

- Any redirection of subnets to Sourcefire is subject to review and approval by the Change Advisory Board (CAB).
- Additionally, any significant changes in Sourcefire policy rules are also subject to Change Advisory Board Approval.
- Access Policies and Access Control Rules were created overtime to leverage Sourcefire IPS, Web Reputation, and AMP (Advanced Malware Protection).

Access Policy and Access Control Rules:

- Access controls rule can be defined based one or more of the following:
  - Zones – For example, Internal and External
  - Networks – Source and Destination Hosts and Subnets
  - Vlan tags
  - Users
  - Applications
  - Ports
  - URL's.

Access Policy and Control Rules:

Enabled
Insert below rule 2
Allow
IPS: no policies Variables: n/a Files: no inspection Logging: no logging
Allow
Trust
Monitor
Block
Block with reset
Interactive Block
Interactive Block with reset
lications Ports URLs Inspection Logging
lable Applications (3296)
Search by name
Selected Applications and Filters (0)
any
Very Low 1111
Low 811
Medium 995
High 214
Very High 123
ess Relevance (Any Selected)
Very Low 812
BackWeb
BACnet
Badoo
Baidu
Baidu Movies
Baidu Yun
BaiduHi
Baiduspider
Balatarin
Add to Rule
Viewing 301-400 of 3296
Add

Access Policy and Control Rules:

w Educational Institutions | Enabled | Insert | below rule | 2

Allow | IPS: *no policies* | Variables: *n/a* | Files: *no inspection* | Logging: *no logging*

Networks | VLAN Tags | Users | Applications | Ports | URLs | Inspection | Logging | C

and URLs

y name or value

er and Internet Security
ed SPAM Sources
Occult
es (db Ops only)
Comment
nal Institutions
nment and Arts
and Beauty
Services

Reputations

Any
5 - Well Known
4 - Benign sites
3 - Benign sites with security risks
2 - Suspicious sites
1 - High Risk

Add to Rule

Selected URLs (1)

Educational Institutions (Reputation 5

Enter URL

Add

Access Policy and Control Rules:

For each individual rule, an Intrusion Policy or File Policy (AMP Inspection) can be applied to it.

Editing Rule - Camosun - Test URL Filter

Name: Camosun - Test URL Filter
Enabled
Move

Action: Interactive Block
IPS: Connectivity Over S... **Variables:** Default Set **Files:** Camosun_Wireless **Logging:** connections, files:...

Zones | **Networks** | VLAN Tags | Users | Applications | **Ports** | **URLs** | **Inspection** | **Logging** | **Comments**

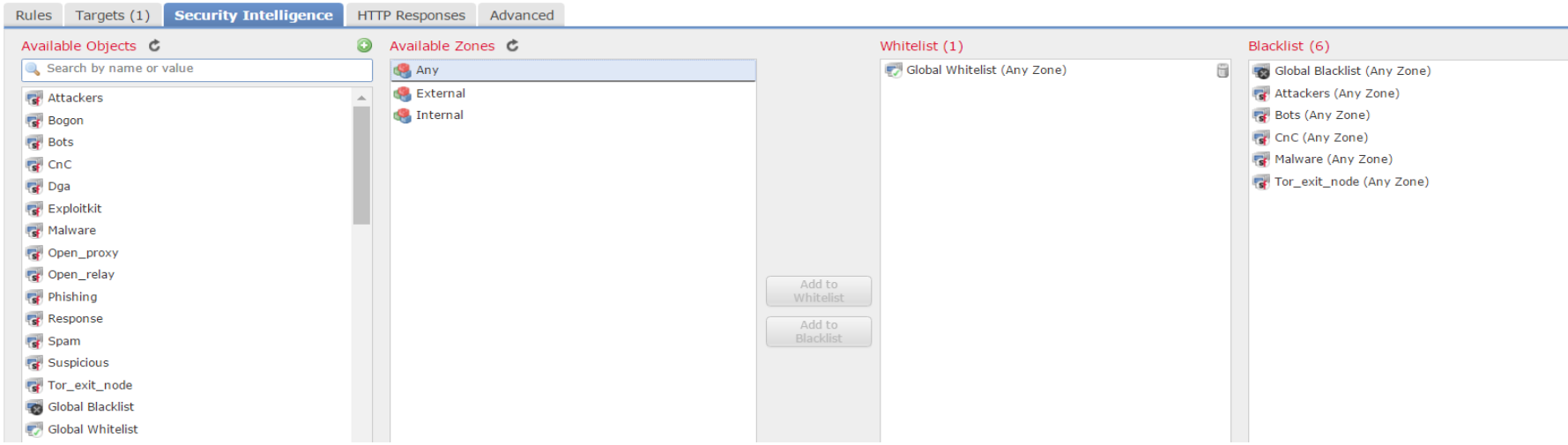
Intrusion Policy: Connectivity Over Security

Variable Set: Default Set

File Policy: Camosun_Wireless

Access Policy and Control Rules:

Additionally, there is a cloud based Security Intelligence feed:

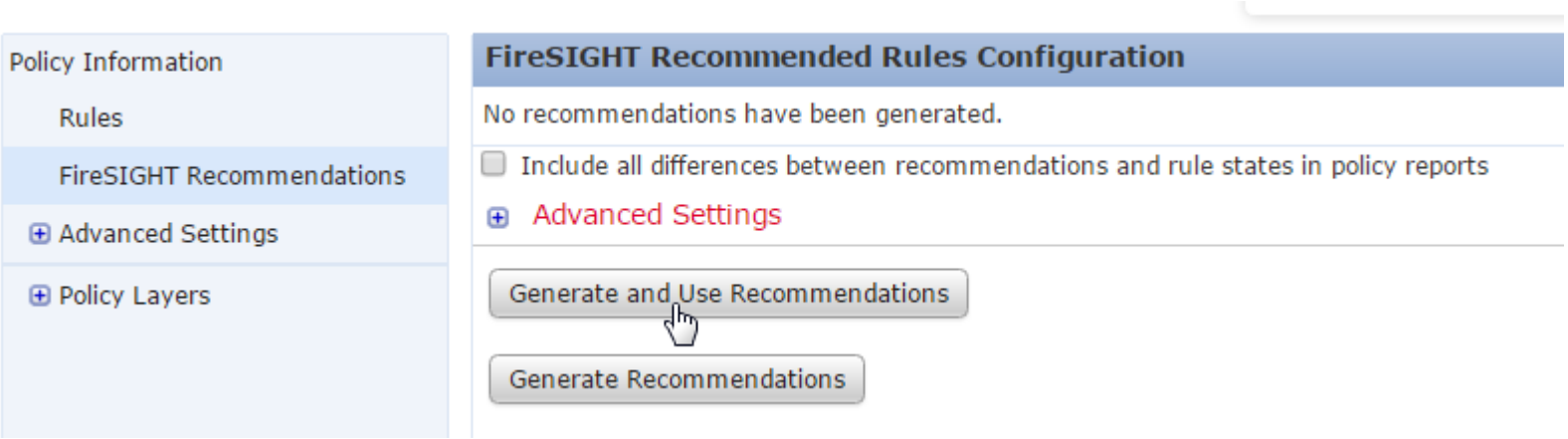


Firepower Management Center.

- Of particular significance is its ability to store relational data about network hosts and users.
- Over time the firepower management center will accumulate data and learn about the hosts on the network. Especially if the host is always configured with the same IP address. In addition to self learning, it is also possible to run nmap scans for services and manually hard code the operating system and application information.

IPS Policy and Automatic Rule Selection

- Based on host data, Firepower has the ability to automatically recommend (enable) rules and generate an IPS Policy.



File Inspection Policy and AMP (Advanced Malware Protection)

- In order to scan for malware a File Inspection Policy is create which can then be applied to an access control rule.

Camosun Wireless File Policy

Rules | Advanced

Used by 3 access control policies | Add File Rule

File Types	Application Protocol	Direction	Action	
Category: Dynamic Analysis Capable Category: System files Category: Graphics Category: Encoded (5 more...)	Any	Any	Malware Cloud Lookup Store files of disposition: Malware	

Generate Recommendations

AMP (Advanced Malware Protection)

- When a file is inspected the name of the file, session details are logged along with a SHA256 hash.
- Using the SHA256 hash as an identifier, the file reputation can be referenced.

- *** Additionally, if a file at later time is categorized as malware, then you have the ability to run a report and identify the recipient hosts on your network.

AMP (Advanced Malware Protection)

- The following is a sample e-mail alert received due to a network based retrospective event:

- <*- Network Based Retrospective at Fri Mar 10 12:47:37 2017 UTC -*>
- Sha256: d42ed32ee21917e98512f5581d59d28693c89b9a13b047b9d0ed8861bf5675a8
- Disposition: Malware
- Threat name: N/A

- <*- Network Based Retrospective
- From "192.168.131.250" at Thu Mar 9 20:05:51 2017 UTC -*>
- Sha256: d42ed32ee21917e98512f5581d59d28693c89b9a13b047b9d0ed8861bf5675a8
- Disposition: Malware
- Threat name: N/A
- IP Addresses: 192.168.1.2<-69.192.84.59

- <*- Network Based Retrospective
- From "192.168.131.250" at Thu Mar 9 16:16:24 2017 UTC -*>
- Sha256: d42ed32ee21917e98512f5581d59d28693c89b9a13b047b9d0ed8861bf5675a8
- Disposition: Malware
- Threat name: N/A
- IP Addresses: 192.168.1.3<-104.125.248.101

AMP (Advanced Malware Protection)

- Additionally, it is possible to submit files to a cloud based resource for further “sandboxed” inspection. The file is executed and analyzed, and a report is generated.
- The following website is also particularly useful for researching detected malware:
  - http://www.virustotal.com

- AMP is also available for other products such as Cisco Integrated Services Routers

Cisco AMP for Endpoints

- Cisco Amp for Endpoints provides endpoint security for PCs, Macs, Linux Systems, and Mobile Devices.

- Cisco AMP for Endpoints integrates with Firepower Management Center. Endpoint can also potentially be a better solution than ssl decryption and AMP inspection on a FirePOWER module.

Web Reputation / URL Categorization

- This is subject to change, but currently Sourcefire relies on Webroot “BrightCloud Threat Intelligence”.
- The following URL is useful to lookup a risk rating or categorization for an IP address or URL:
  - http://www.brightcloud.com/tools/url-ip-lookup.php
- Currently, other vendors such as F5 and Palo Alto utilize BrightCloud Threat Intelligence. (Please correct me if this is no longer valid)

Firepower Management Center Insight via Dashboards, Analysis, Reports, and Alerting

As Firepower appliances are added to the main campus network and to remote “satellite locations”, the Firepower Command Center provides a “single pane of glass” or single location to view the current status of the network and any detected threats.

Firepower Management Center Insight via Dashboards

The following dashboards are available:

- Application statistics
- Connection Summary
- Detailed Dashboard
- Files Dashboard
- Summary Dashboard
- URL Statistics

Firepower Management Center Analysis

Firepower Management Center offers numerous analysis / query options (I could spend a day discussing analysis options).

To summarize:

- Context explorer
- Connection and Security Intelligence Events
- Intrusion Events
- File Malware events and File Trajectory
- Host and User information
- Vulnerability Information

Camosun - Future Firepower Work

- Upgrade to Firepower version 6.2
- Deploy more ASA 5506-X appliances…In the past year, we have been deploying the new ASA 5506-X appliance (future replacement for ASA 5505 models).

- All 5500-X appliances have a permanent AVC (Application Visibility and Control license).
- The ASA 5506-X model is the smallest and most affordable appliance to deploy to smaller remote satellite locations. They are typically configured with split VPN tunnel configurations.
- All of the ASA 5506-X units will be configured to connect to the central Firepower Management center.
- Test Firepower Thread Defense

Firepower Threat Defense

- Firepower Threat Defense (FTD) is a unified image of the ASA and Firepower. This unified image can be centrally managed via the Firepower Management Center.
- The current ASA software will inevitably be replaced by FTD. However, features such as the Cisco Anyconnect VPN client are not currently available.
- The ASA with Firepower services combination does have the ability to “fail open”. This means that if desired a Firepower module can be upgraded without impacting network traffic. However, it also means that there is no protection available during a Firepower software upgrade.

In summary

- The implementation of Sourcefire (aka Firepower) at Camosun College has significantly improved network services and has provided an additional layer of protection for faculty, staff, and student systems.
- More work is still entailed to achieve a balance between network access and security. However, Sourcefire/Firepower is a powerful tool. Especially, when setting a policy for unmanaged BYOD systems and applications.
- AMP - Advanced Malware Protection has already paid for itself by identifying threats that other software vendors cannot identify. Additionally, the retrospective capability of AMP, allows for quicker identification and remediation of systems identified with Malware.