SAFE Design Guide

Security Domain: Threat Defense

Use Case: Cisco Ransomware Defense

Added Advanced - Updated August 2017

Contents

Introduction 4
Overview 5
Ransomware infection 6
Common vectors of infection into an organization 6
Ransomware communications 7
Ransomware kill chain 8
Ransomware defense 9
Best practices 10
Things you can do 10
Recovery in the event that the worst has happened 11
Solution Architecture 11
Phase One—Quick prevention 13
Email security 13
DNS security 15
Anti-Malware security 16
Threat Intelligence 17
Phase Two – Detect and contain ransomware 18
Advanced web security 19
Network monitoring 20
Identity-based segmentation 20
Infrastructure segmentation and intrusion prevention 20
Architecture summary 21
Implementation Phase 1—Quick Prevention 22
Cisco Cloud Email Security 22
Cisco Umbrella DNS security 30
Cisco Advanced Malware Protection for Endpoints (AMP) 36
Implementation Phase 2 advance solution 40
Cisco Identity Services Engine (ISE) 41
Configuring network authentication 41
TrustSec 47
ISE policy matrix 47
Security Group Tag Exchange Protocol 48
Firepower Threat Defense (FTD) Policy 60
Stealthwatch 63

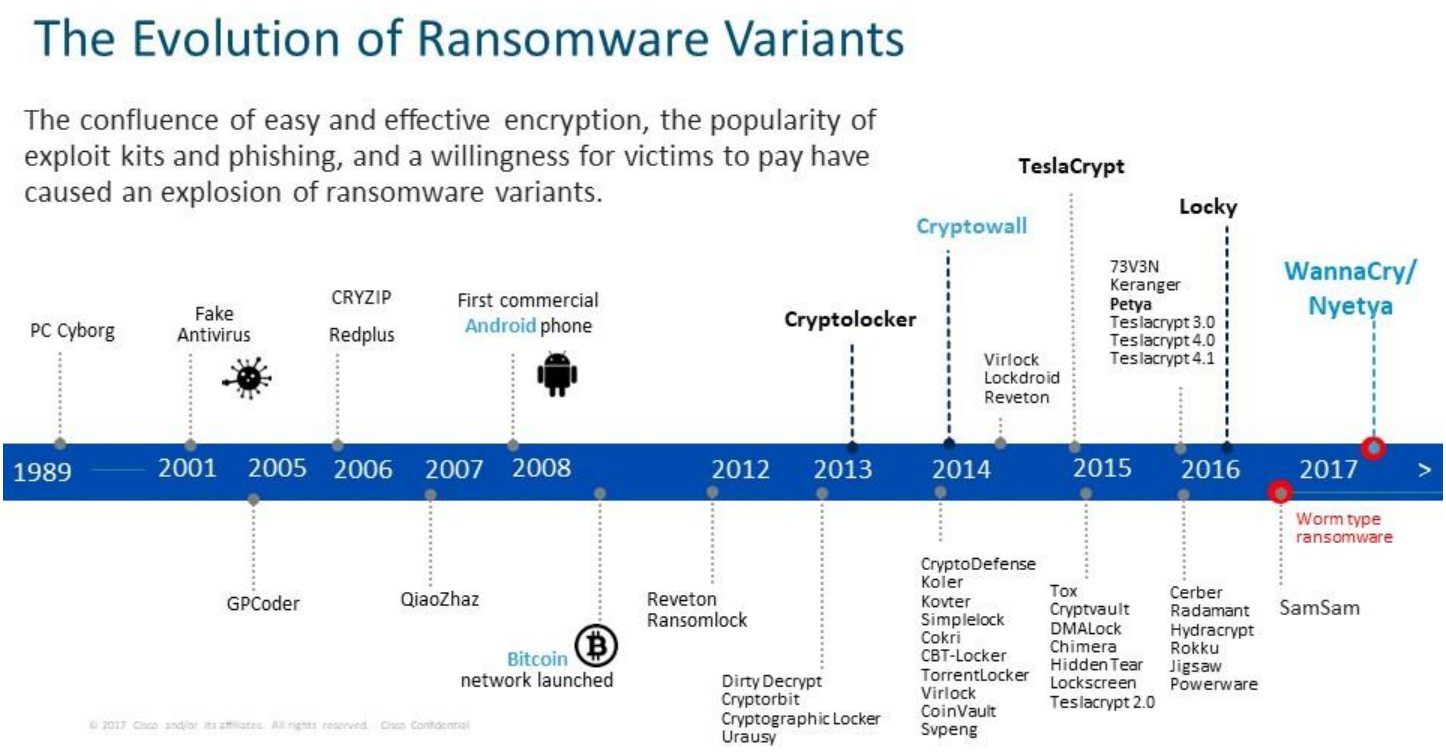
Cisco Stealthwatch with Threat Intelligence 63
Better Visibility and Contextual Threat Intelligence 63
Stealthwatch and ISE integration 64
Validation Testing 66
Advanced Ransomware Solution Validation Testing 67
Solution component implementation 67
Testing objective 68
Testing setup and each component role 68
FTD and ISE 68
ISE and TrustSec 68
ISE and Stealthwatch 68
Network Topology 69
Validation Testing 70
Summary of Tests Performed 70
Summary of results 71
Summary of results 71
Summary 71
References 72

Introduction

Ransomware is the most profitable type of malware in history. In the past, malware typically did not deny access to systems or destroy data. Attackers primarily tried to steal information and maintain long term access to the systems and resources of their victims. Ransomware has changed the game from stealthy undetected access to extortion.

Every single business or person who pays to recover their files makes this payment directly to the attackers. The relatively new emergence of anonymous currencies such as Bitcoin and Ripple gives attackers an easy way to profit with relatively low risk, making ransomware highly lucrative and funding the development of the next generation of ransomware. As a result, ransomware is evolving at an alarming rate. Recent ransomware attacks propagate like worms, spreading throughout an organization in a coordinated manner; and aggregate the ransom demand or aim to cause business disruption and destruction regardless of the ransom payout.

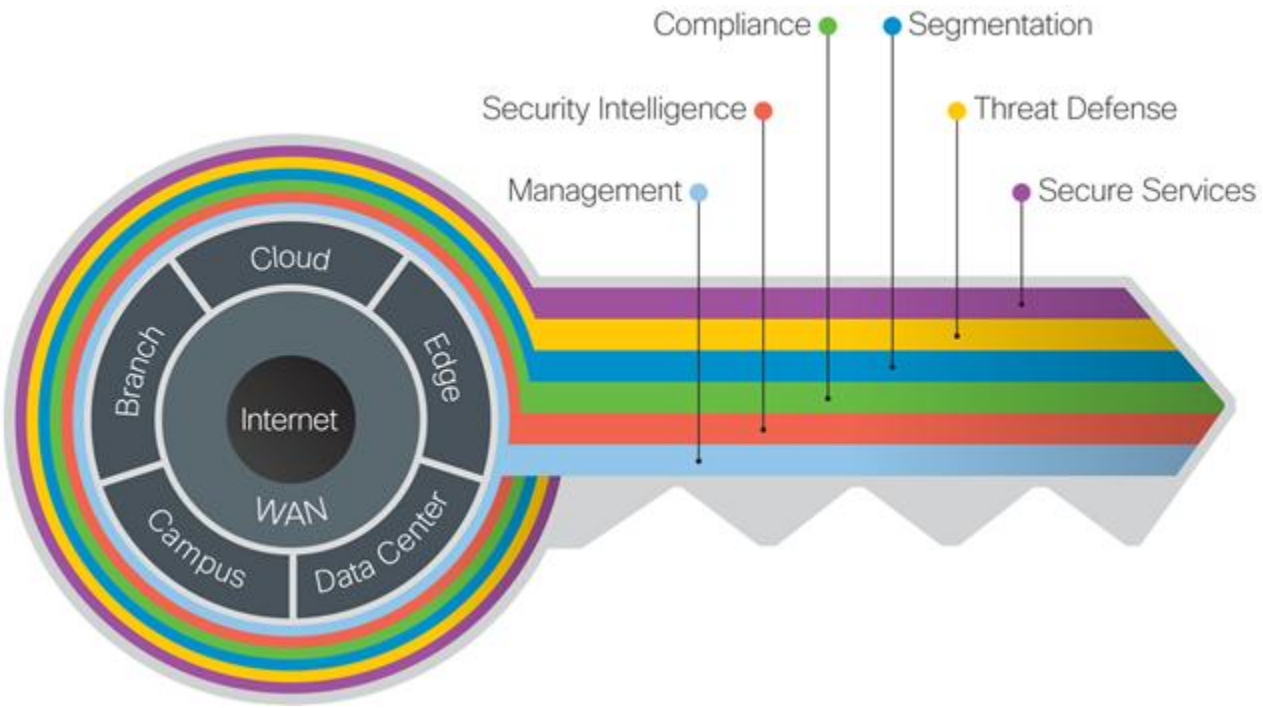
Figure 1 – The Evolution of Ransomware Variants



Cisco can help protect your business from the ransomware threat using a defense in depth architectural approach. This approach protects users both inside and outside the network.

This guide addresses a specific use case of ransomware under the SAFE Threat Defense domain. This guide includes a recommended ransomware defense architecture for the Campus PIN. SAFE simplifies complexity across the enterprise by implementing a model that focuses on the areas that an organization must secure. This model treats each area holistically, focusing on today's threats and the capabilities needed to secure each area against those threats. Cisco has deployed, tested, and validated these critical business challenges. These solutions provide guidance, complete with configuration steps that ensure effective, secure deployments for our customers.

Figure 2 – SAFE Threat Defense



The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains.

Ranging from business flows and their respective threats to the corresponding security capabilities, architectures and designs, SAFE provides guidance that is holistic and understandable.

More information about how Cisco SAFE Simplifies Security can be found here: www.cisco.com/go/safe

Overview

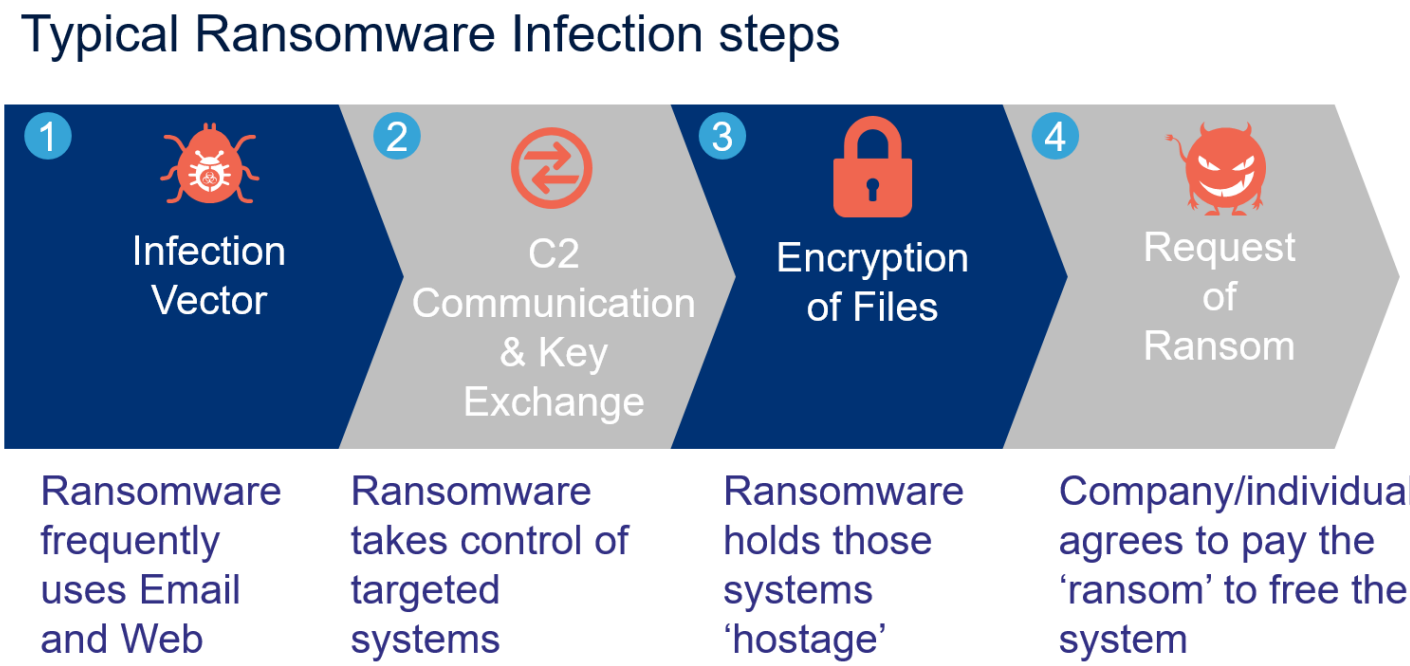
Businesses and individuals can be taken hostage by malware, called ransomware, that locks up critical resources. Ransomware uses traditional malware attack vectors such as phishing emails, known vulnerabilities, and exploit kits to deliver the ransomware to a desktop. Once established, it takes over systems and stored data, encrypting their contents, denying access, and holding them hostage until a ransom is paid. During this time, ransomware also spreads throughout the network, causing significant business disruption. Ransomware uses well-established public/private key cryptography which leaves the only way of recovering the files being the payment of the ransom, or restoring files from backups. Currently, it is understood that If the ransom demand is paid, the attacker often, but not always, provides the decryption keys to restore access.

The denial of access to these critical resources can be catastrophic to businesses:

- Hospitals can lose the ability to give patients real-time care (admittance, surgeries, medications, etc)
- Manufacturers can have product downtime and miss shipping/delivery schedules
- First responders can be prevented from responding to 911 or emergency calls
- Financial banking systems can be offline for trading or banking activities
- Retail outlets cannot process payments and customers cannot make purchases

Ransomware infection

Figure 3 – Typical Ransomware Infection Steps



1. Ransomware is commonly delivered through mass phishing campaigns, malvertising, or targeted exploit kits.
2. After delivery, ransomware takes control of your system and may try to communicate back to its command and control infrastructure to create and transmit the public/private keys used to encrypt the files.
3. Once the ransomware has the necessary keys, it identifies specific file types and directories to encrypt, and avoids many system and program directories, ensuring stability for delivery of the ransom after it finishes running.
4. After encryption completes, a notification is left for the user with instructions on how to pay the ransom.

Common vectors of infection into an organization

There are many ways an organization can be compromised by ransomware; the most common are e-mail phishing attacks and web hosted malvertising.

Email: E-mail is a one-to-many infection vector when used with distribution lists and mass mailings. It is common for a single user to manage multiple email accounts both personal and corporate. Every account represents a security threat. For example, although IT organizations spend enormous time and effort to select mail security services such as Cisco Email Security Appliance or Cloud, it is very common for the users to check their personal email using public email services such as Hotmail and Gmail. These private email accounts are easily accessed through web portals that bypass these email security services. Accessing, downloading, and executing email attachments and phishing links from such accounts are a major concern.

Web: Malvertising ads are criminally-controlled adverts that intentionally infect systems installing exploit kits or ransomware directly. These can be any ad on any site, and are often sites accessed on a daily basis. When a user clicks on the ad, they are taken to a site that then infects their computer. Malvertisement networks comprise thousands of network domain names, creating a shared

infrastructure that is constantly changing. These domain names can be random or semi-structured, but all have a relatively short lifespan, being replaced frequently. These domains host the exploit kits, tools, and command and control services criminals use to infect, control, and disrupt systems. Almost all of these communications are encrypted.

There are multiple ways that users can interact with malvertising, such as simply visiting a site that serves ads or clicking on a link in a page of search results or an email[1]. Savvy web surfers often implement adblockers on their systems for protection, but this can impact a site's ad revenue, so there is a battle restricting content and requiring adblocks to be disabled. Although major sites can limit access to their site based on the use of an adblocker, these publishers cannot guarantee that the ads served will not be malicious. These sites and services are prime targets for compromise and redirection.

Ransomware is aggressively evolving to adopt the most invasive features of other malware (e.g., Nimda, Sasser, Code Red, SQL Slammer, Sality, Conficker), spreading and infecting an entire enterprise network, encrypting all the data they can access for a larger lump-sum payout, or spread the malware throughout the network and cause significant disruption.

Ransomware communications

Ransomware communications include command and control (C2) callback methods for obtaining encryption keys and payment messaging, as shown in table 1.

Table 1 - Ransomware Communication Methods

	Encryption Key				Payment Msg
NAME*	**DNS**	**IP**	**No C2**	**TOR**	**Payment**
Locky	✓	✓			DNS
SamSam			✓		DNS (TOR)
TeslaCrypt	✓				DNS
CryptoWall	✓				DNS
TorrentLocker	✓				DNS
PadCrypt	✓				DNS (TOR)
CTB-Locker	✓			✓	DNS
FAKEBEN	✓				DNS (TOR)
PayCrypt	✓				DNS
KeyRanger	✓			✓	DNS

*Top variants as of March 2016

[1] http://blog.talosintel.com/2016/05/spin-to-win-malware.html

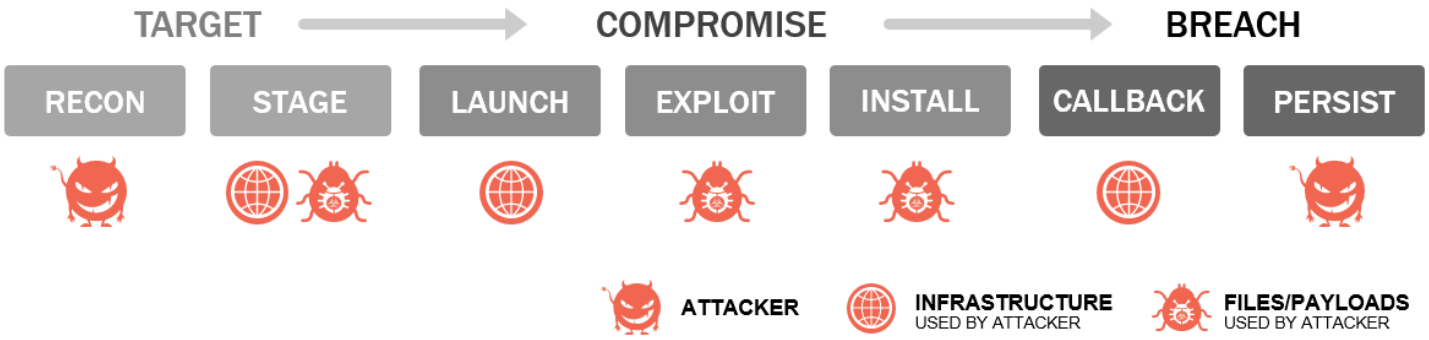
Once a system is successfully compromised, the exploit kit analyzes its environment (e.g., OS, unpatched applications, etc.) to then retrieve and drop an effective ransomware variant. A callback is then made to the ransomware infrastructure to retrieve the keys needed to encrypt the system. Many of the most prevalent exploit kits and ransomware variants resolve a domain name to an IP address to initiate this callback.

Although some variants of ransomware behave differently — for example, SamSam uses a built-in encryption key that does not require a C2 callback, and other variants use Tor-based Onion Routing or IP-only callbacks that avoid DNS — there are many ways that the Ransomware Defense Solution can help.

Ransomware kill chain

The first two steps of the infection process outlined above are most commonly broken down into seven stages of an attack, as shown in Figure 4. Not all attacks use every stage, but these are the most common.

Figure 4 - Seven stages of an attack



The term “Kill Chain” refers to the ability to block an attack at any of these specific stages if the correct capabilities can be employed. Below is a brief description of these stages as they are commonly understood across the security industry by similar names[2].

RECON: The attacker gathers information to help them create seemingly trustworthy places and messages to stage their malvertisements and phishing emails.

STAGE: Using information collected during RECON, the cybercriminals try to fool users into opening e-mails or clicking on links.

LAUNCH: The staging sites redirect from “trustworthy” looking sites to sites that launch the exploit kits and/or other malicious content.

EXPLOIT: Once a user is at the compromised site, their system is scanned for vulnerabilities that are then exploited to take control of the user's system.

INSTALL: Once an exploit has taken control, the final dropped file/tool is installed that infects and encrypts the victim’s system; this is the ransomware payload. This stage may also include additional executables to deliver other malware in the future.

CALLBACK: Once infected, it “calls home” to a command-and-control server (C2) where it retrieves keys to perform the encryption or receive additional instructions.

PERSIST: The files on the hard disk, mapped network drives, and USB devices are encrypted and a notice or splash screen pops up with instructions to pay the ransom to restore the original files. This notice persists, and at times deletes files, as a timer counts down to the expiration of being able to retrieve the unlock keys, putting extreme

[2] http://www.cisco.com/c/en/us/products/security/annual_security_report.html

pressure on the user. Additionally, the attacker's exploit kit can persist and pivot to other more critical systems.

Ransomware defense

The Ransomware Defense Solution creates a defense in depth architecture with Cisco Security best practices, products, and services to prevent, detect, and respond to ransomware attacks. Cisco's Ransomware Defense Solution is not a silver bullet or a guarantee, but it does help to:

- Prevent ransomware from getting into the enterprise wherever possible
- Stop ransomware at the system level before it gains command and control
- Detect when ransomware is present and spreading in the network
- Work to contain ransomware from expanding to additional systems and network areas
- Performs incident response to fix the vulnerabilities and areas that were attacked

This solution helps to keep operations running, reducing the fear of being taken hostage and losing control of your critical systems.

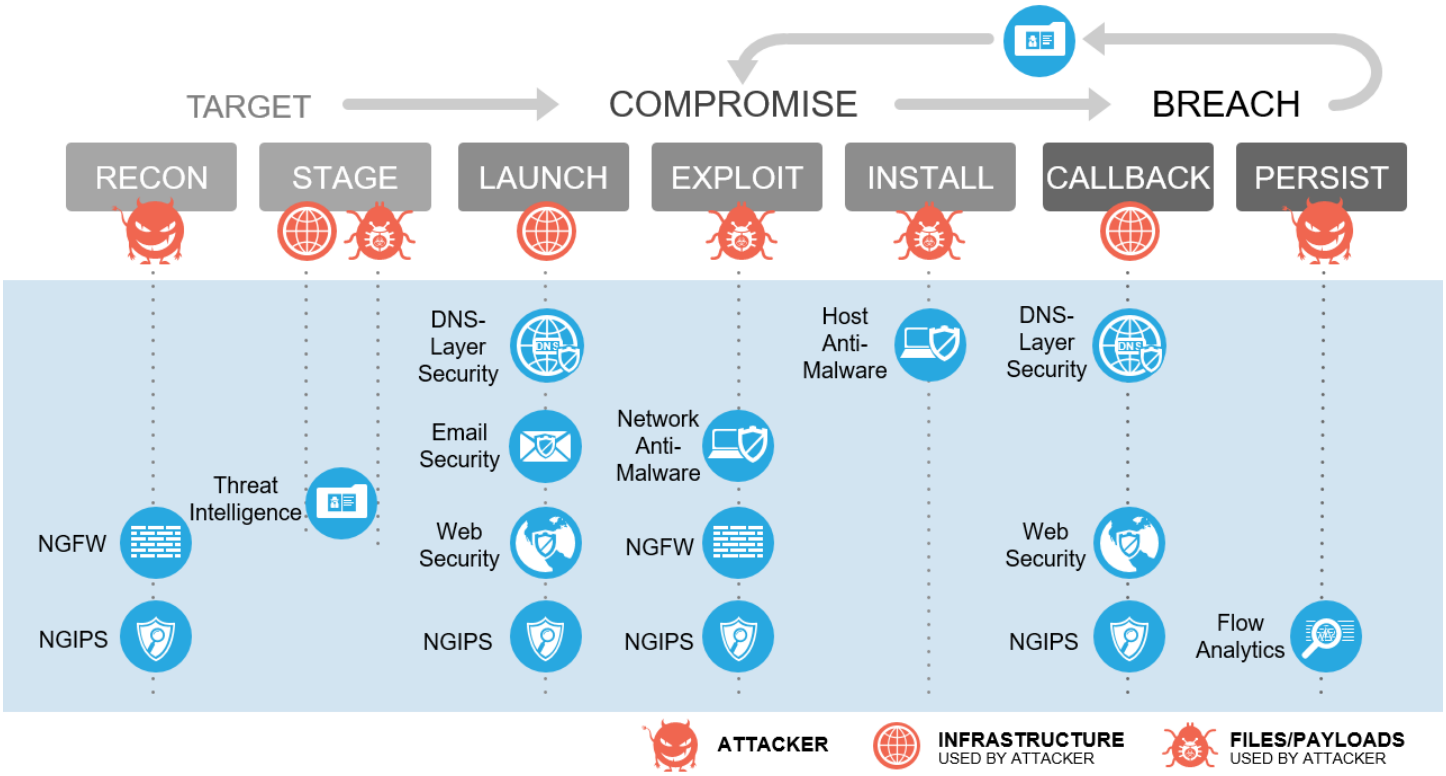
To defend against the ransomware kill chain, specific capabilities are necessary to build the appropriate layers of defense. Table 2 identifies the SAFE methodology capabilities (Blue Circles) best suited for this defense.

Table 2 - Safe capabilities to defend against ransomware attacks

icon	Capability	Function
	Threat intelligence	Knowledge of existing ransomware and communication vectors, and learned knowledge in new threats.
	E-mail security	Block ransomware attachments and links
	DNS security	Block known malicious domains and break the command and control callback
	Client security	Inspect files for ransomware and viruses, and then quarantine and remove
	Web security	Block web communication to infected sites and files
	Identity-based firewall segmentation	Authenticate access, separate traffic based on role and policy
	Intrusion prevention	Block attacks, exploitation, and intelligence gathering
	Network monitoring	Monitor infrastructure communications using flow-based analytics – Identify and alert on abnormal traffic flows

Each of these capabilities are then deployed to combat and defend against the seven stages of an attack, as shown in Figure 5.

Figure 5 - Breaking the kill chain with security capabilities



These capabilities work together to create several layers of defense, protecting the organization against the threat and spread of ransomware.

Best practices

Things you can do

It is not enough to have a world-class defense in depth architecture. You need to know what the critical priorities are in running your business, and whether they can be impacted if your systems are locked down.

- The most important action is to ensure that you have good backups and that you test the backup system for effectiveness. If you do weekly backups, transition to daily; if you do daily, look to transition to hourly or real-time. Some backups enable a roll back to a state before the attack occurred. This can be useful in some environments, but may not help with others.
- Develop a good disaster recovery plan, and ensure that it is regularly tested and updated as the business grows and changes.
- Know to whom to make the ‘first call’. When an employee is hit with ransomware, who are they going to call first? Many times it is the IT dept, but not always. Ensure the ‘first responder’ knows what actions they should take and can respond quickly
- Identify all of the people, processes, and tools necessary to handle a critical disruption or event. Perform drills to test these plans on a regular basis.

- Develop a comprehensive baseline of the applications, system images, information, and your normal running network performance. These give you visibility into changes on your network, enabling detection of the unusual.
- Standardized images of operating systems and desktops allow for easy re-imaging to recover infected infrastructure.

Recovery in the event that the worst has happened

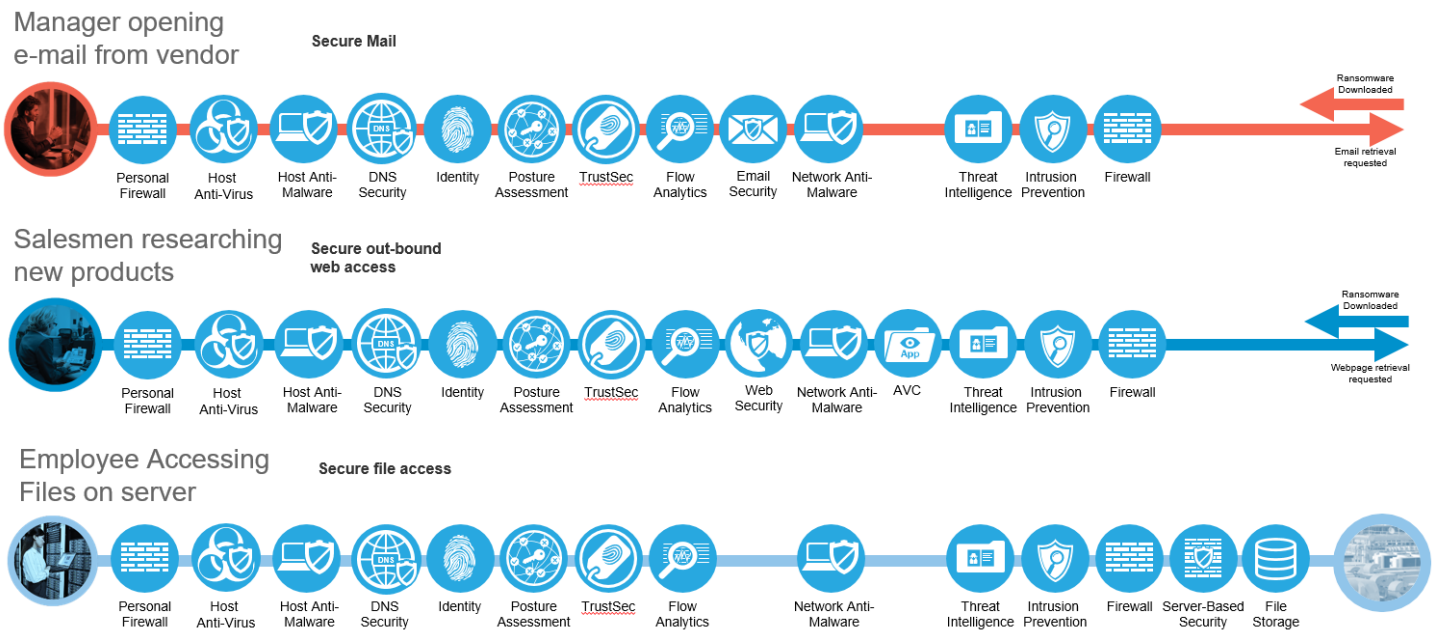
Backup recovery is your last line of defense, and avoids having to pay out a ransom to the attackers. Your ability to recover from this attack with minimal data loss and/or service interruption amounts to whether or not the system backups and/or disaster recovery sites were compromised as a part of the attacker methodology. Whether or not your backups were compromised depends on how well your backup systems and/or network and/or recovery sites were sufficiently segmented from your main network. Even in the event your organization does not use on-site backups at all, instead opting for cloud backup solutions (e.g., Amazon Glacier), if those cloud backup credentials are left in easily accessible locations, or if passwords are reused, the attacker could easily delete all backup instances, resulting in 100% data loss if there is no other backup solution in place. A secure, off-site, enterprise backup solution could easily be defeated through password reuse and/or poor password management.

For enterprises using backup solutions, there are a wide variety of backup methodologies; the SANS reading room has a comprehensive document on tape rotation schemes that is incredibly helpful. Typically, as a part of a tape rotation policy, a portion of these tapes are delivered to an off-site storage facility. This is for disaster recovery purposes; if there a catastrophic failure at the site hosting an organization's data, the tapes at the storage facility are still there to recover from at a backup facility. In a scenario in which local backups are deleted, removed, or otherwise made inaccessible by the attackers, off-site backups are often your only hope of restoring service without paying the ransom. Depending on how often your backups are sent off-site determines how much data (if any) would be inaccessible or lost.

Solution Architecture

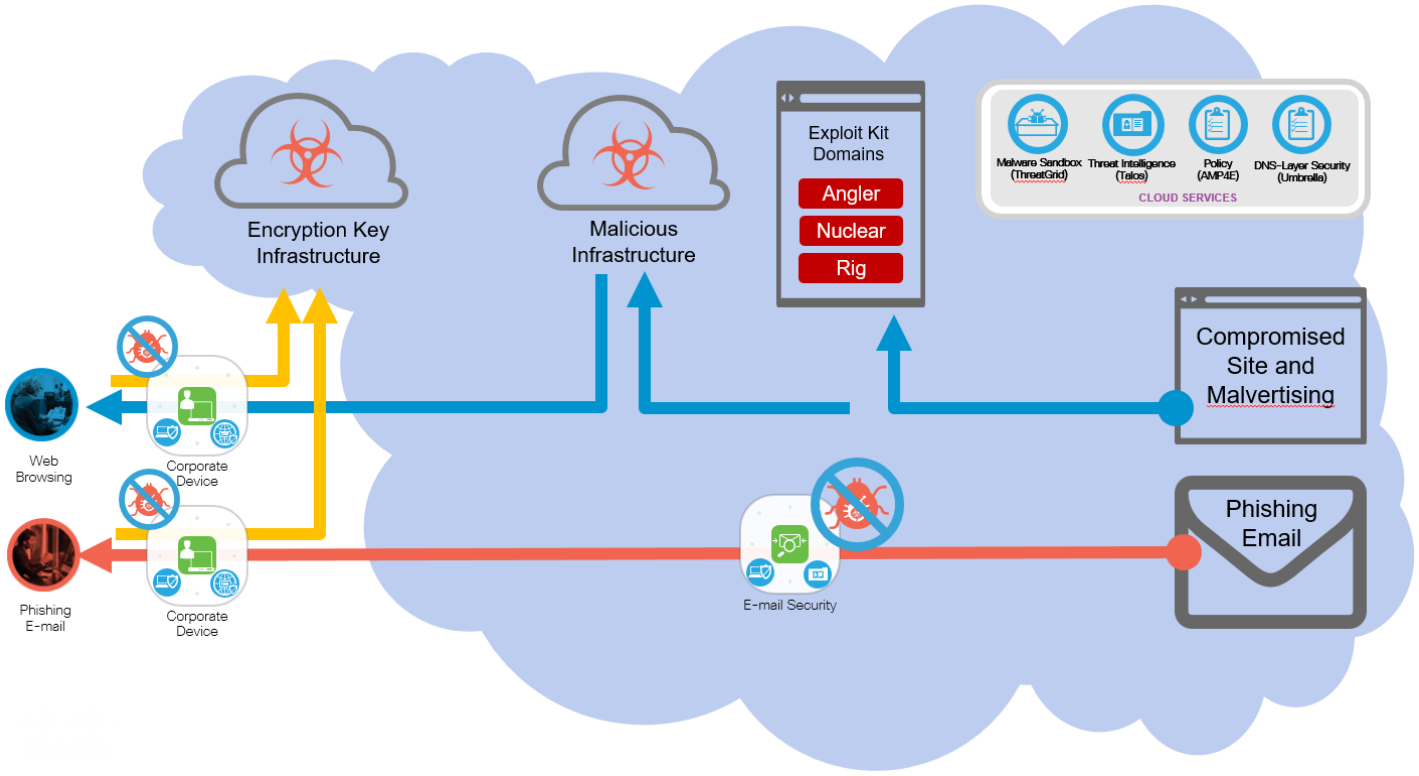
The first step in developing a defense in depth architecture is to take all of the capabilities that can break the ransomware kill chain and match them up with the real world business functions/flows as identified in the SAFE model. Specific to ransomware, these are web browsing and email usage, as these are the highest risk methods of infection. Also included are files on internal storage as a third example. Each of these three business flows are shown in Figure 6, with the selected capabilities described above. Across an organization, these capabilities may be duplicated in several PINS. All duplicates have been removed, and the capabilities are not necessarily in any specific order. They are just representations of the best ways to protect the flows from and end-to-end perspective.

Figure 6 - SAFE business flows and capabilities



Because a comprehensive deployment of these capabilities can include significant costs and time to deploy, this solution has been divided into two phases. Phase one includes several capabilities that can be rapidly deployed with relatively low effort and achieve a great reduction in risk, as shown in Figure 7. Phase two adds the remaining capabilities, and is shown on an example campus network PIN architecture.

Figure 7 - Cloud and endpoint capabilities



Phase One—Quick prevention

With the threat of ransomware attacks and infections looming, action must be taken to block them before becoming the next victim. The organization must augment existing security measures by implementing email, DNS, and anti-malware security capabilities. These are quick and easy-to-deploy cloud-enabled services that provide an immediate reduction in the risk of successful ransomware attacks.

Three steps to a quick and successful defense include;

1. Block the number one vector of infection—Filtering email attachments and URLs before they reach a single user (Cisco email security).
2. Stop command and control (C2) communication, and redirection to malicious sites—Add a layer of DNS security (Umbrella) for on-net and off-net protection.
3. Enable malicious file protection (AMP) capabilities across all supporting infrastructure (hosts, network, email, and web).

Deploying these capabilities is crucial, and should be prioritized by group; admins, executives, key servers, and then as broadly as possible.

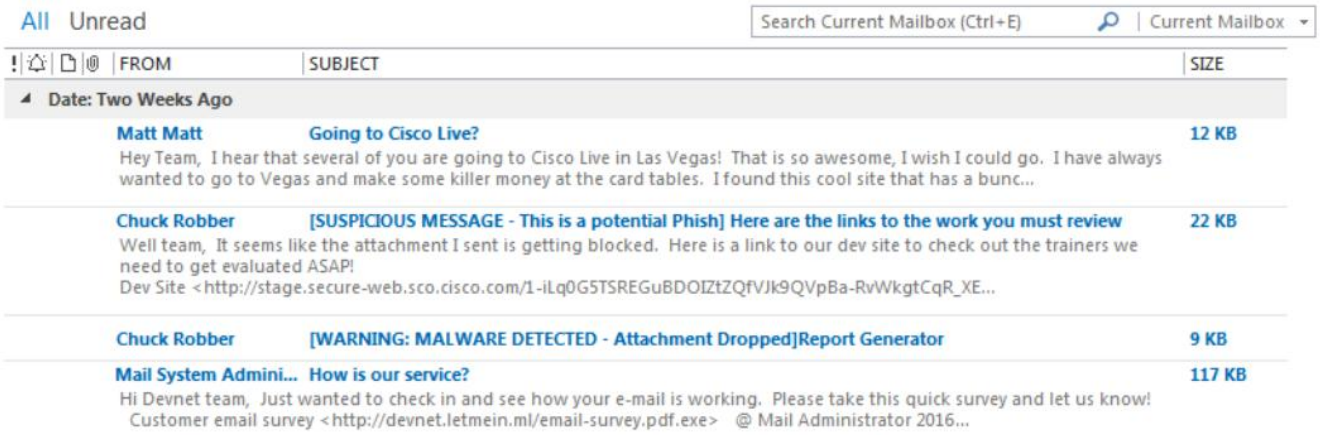
Each of these offerings share the cloud-based services of Talos Threat intelligence, Threat Grid file analysis and Umbrella Security Graph.

Email security

Email security blocks a significant amount of ransomware attacks by pre-filtering all messages coming into an organization (red arrow from Figure 7) before ever reaching a real person that may open or click on it. Messages are evaluated through several policy enforcement inspection steps, which must be enabled. These include content, virus checking, malware checking, and spoofing. Malware checking is performed using the Advanced Malware Protection (AMP) integrated service; known bad attachments (based on file hashes and other recognition abilities) can be stripped, but the best practice is to drop or quarantine the entire message. For unknown attachments, messages are held in a quarantine while the attachments undergo file analysis in the Threat Grid file sandboxing service. Forwarding decisions are then chosen based on the severity of the analysis report returned. Proper Cloud Email Security (CES) integration with mail systems can allow retrospection to clean up infected e-mail before it is retrieved by other users. Figure 8 shows messages with attachments stripped.

NOTE: On rare occasions, malicious files can initially be classified as “safe” because of their ability to change behavior after analysis.

Figure 8 - Email with prepended subject notifications



The email system also evaluates URLs to determine whether a message contains spam or phishing links, and based on the URL's reputation, take an appropriate action. For enhanced protection against ransomware, message modification and virus outbreak filters must also be enabled globally and added to the mail policies. Outbreak filters defend against emerging threats and blended attacks. They can issue rules on any combination of six parameters, including file type, file name, file size, and URLs in a message.

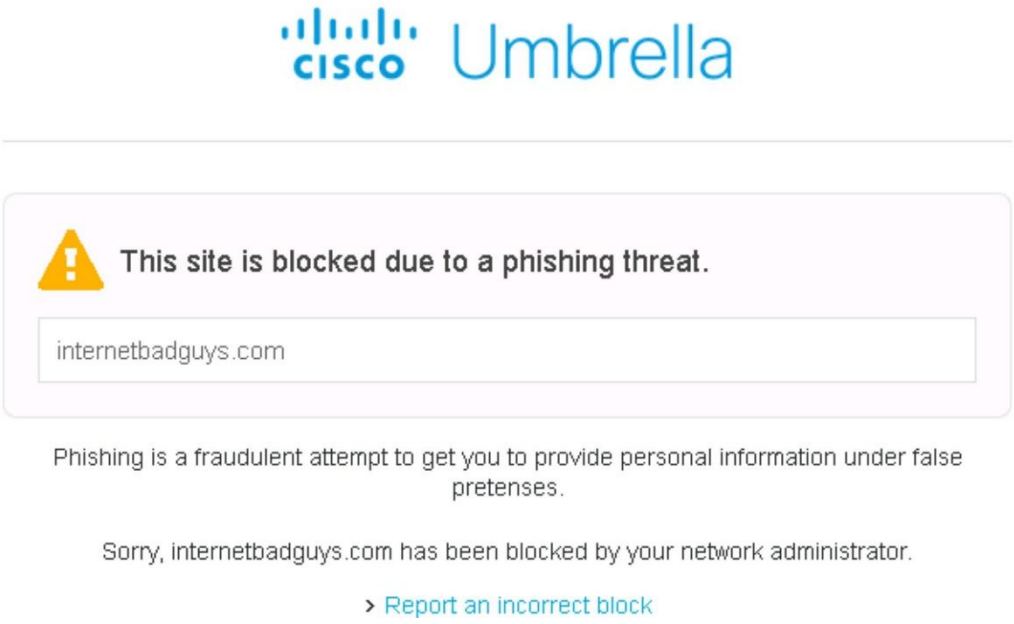
As Cisco's Talos threat Intelligence learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Outbreak filters can also rewrite URLs in suspicious messages. This recipient browsing activity can be tracked by enabling Web Interaction Tracking (WIT). When clicked, the new URLs redirect the recipient through the Cisco Web Security proxy. The website content is then actively scanned, and outbreak filters display a block screen to the user if the site contains malware or exploit kits that could drop ransomware. If the content is unknown, a decision option is presented, as shown in Figure 9.

Figure 9 - Decision option from Web Interaction Tracking

DNS security

DNS security enforces security at the domain name resolution step of converting a name to an IP address to reach a server on the internet. Security at this DNS layer enables the ability to protect devices both on and off of an organization's network for all communication types, not just web sites. In the case of the initial launch where a URL would take a user to a seemingly trustworthy site, Umbrella blocks the DNS request and replaces it with a safe destination before the user's' browser connects to the malicious site—whether the user clicked on a link or if there was a redirect from a compromised site, as shown in Figure 10.

Figure 10 - DNS block page

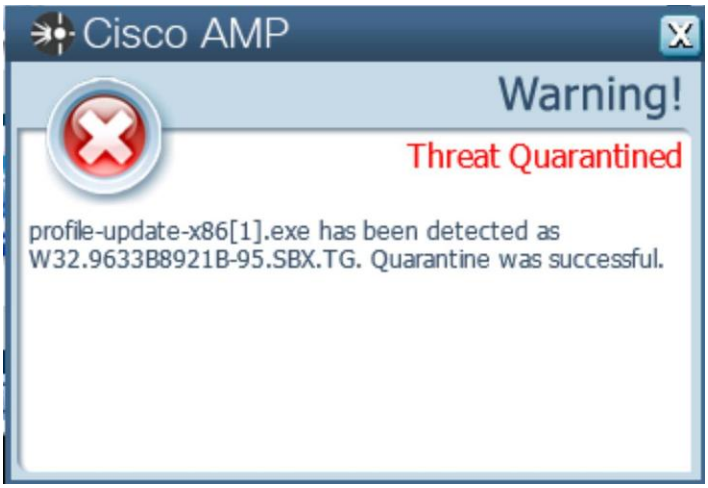


Referring back to Figure 7, several different domain networks may exist for each of the kill chain stages (blue arrows), with differing levels of Threat Intelligence gathered for each. A new domain may be used for the initial phishing site, which is only hours or minutes old, whereas the subsequent malicious infrastructures may have days or weeks of known bad history. Each stage offers an opportunity for DNS security to block this communication before the compromise occurs and protect the user from the infection. Additionally, Umbrella also stops C2 callbacks if an infection does occur (yellow arrows), no matter what port or protocol is used. This stops the ransomware file drop or the C2 callback for encryption keys.

Anti-Malware security

Host-based anti-malware is the last line of defense, and often the only defense for communications encrypted end-to-end (password protected archives, https/sftp, chat file transfers, etc.). Cisco's Advanced Malware Protection (AMP) analyzes all files that reach the user's system. If the file is known to be malicious, it is quarantined immediately, as shown in Figure 11.

Figure 11 - AMP quarantine notification

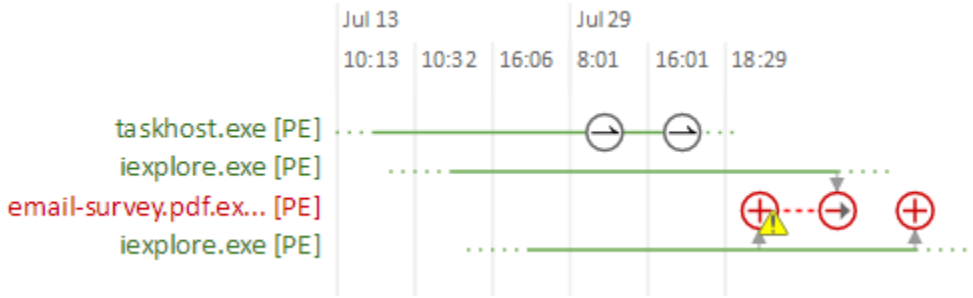


If the file is of low prevalence (files never seen before, and have no history), it is uploaded automatically to Threat Grid for analysis (additional configuration and licensing required) which provides retrospective security to detect malware that evaded initial inspection.

Using a combination of file signatures, file reputation, behavioral indicators, and sandboxing, AMP can stop the initial exploit kit from executing on a user's system and can also stop the execution of the dropped ransomware file and remove it.

Additionally, AMP continuously analyzes and records all file activity on a system, regardless of a file's disposition. If at a later date a file behaves suspiciously, AMP retrospectively detects it and sends an alert. AMP records a detailed history of malware's behavior over time, including where and how it entered the network, where else it traveled, and what it is doing. Based on a set policy, AMP can then automatically or manually contain and remediate the threat. Figure 12 shows how AMP tracks the actions of files on a system.

Figure 12 - AMP device trajectory

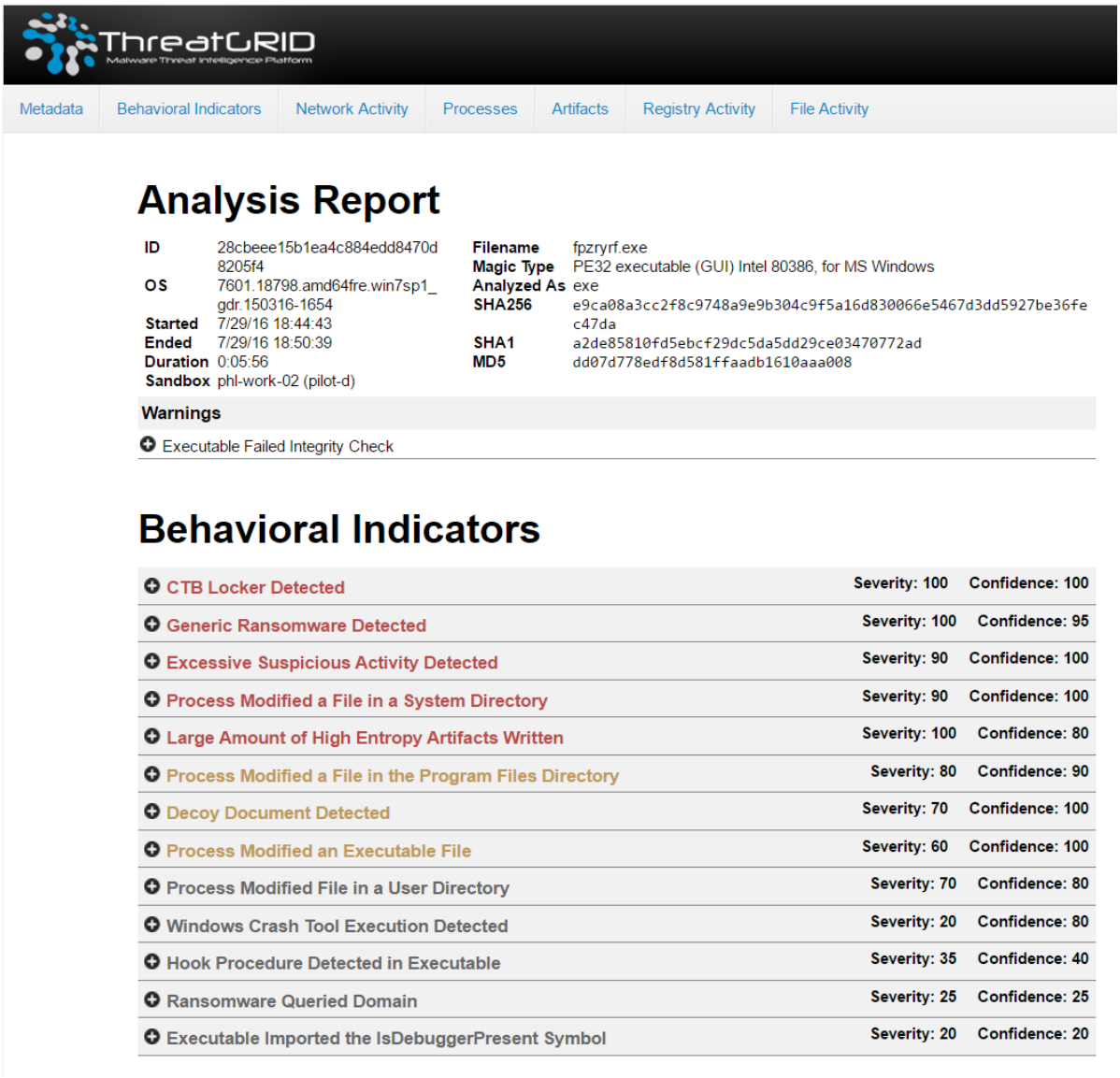


Threat Intelligence

The Cisco Talos Group (Cisco Threat Intelligence Group) analyzes millions of malware samples and terabytes of data per day, and pushes that intelligence to AMP, providing 24/7 protection. Also, advanced sandboxing capabilities perform automated static and dynamic analysis of the unknown files against 500+ behavioral indicators to uncover stealthy threats.

Through the combination of both Talos and Threat Grid threat analysis engines, suspicious email attachments and files can be sandboxed, analyzed, and categorized as malware or ransomware in as quickly as 20-30 minutes. However, low prevalence files may take a slightly longer time to analyze and identify, to minimize the chance of false positives on the analysis. Figure 13 shows an analysis report of a ransomware sample used in the solution validation testing.

Figure 13 - File analysis report

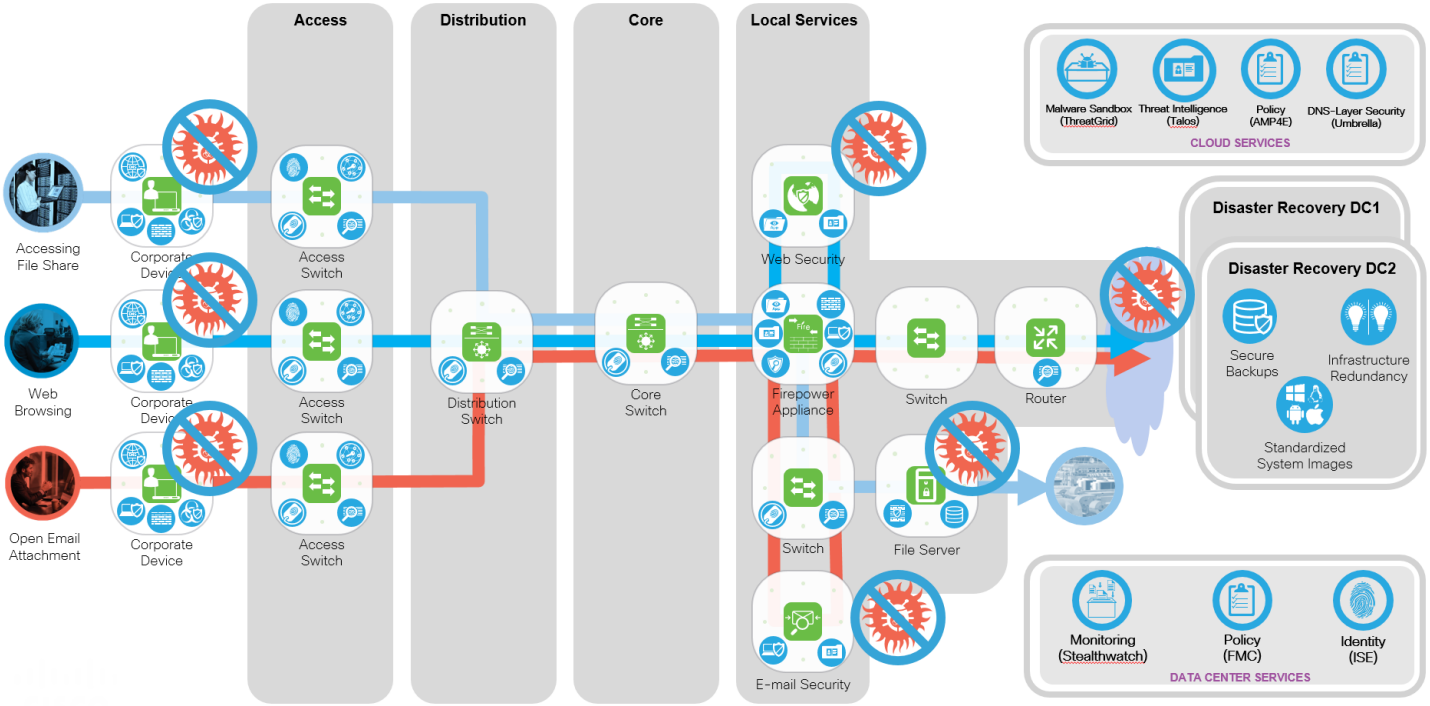


Retrospective security intelligence for malware that evaded initial inspection is shared via Talos Threat Intelligence to both email and host anti-malware services. All current and future instances of these malicious files are blocked or removed.

Phase Two – Detect and contain ransomware

The phase two architecture builds on the capabilities deployed in phase one, implementing a fully segmented role-based infrastructure with network monitoring and enforcement capabilities throughout. Figure 14 shows a sample campus architecture using the SAFE Secure Campus PIN, and layers on the business use case flows of email, web, and file sharing. Each of the capabilities needed to protect these flows are applied to the appropriate system platforms (Green Squares) or shown as cloud services.

Figure 14 - Phase 2 sample campus architecture



Advanced web security

Through web filtering and web reputation scoring, Cisco's Web Security controls access to more than 50 million known websites by applying filters from a list of more than 75 content categories. These controls cover access to web pages, individual web parts, and micro-applications so employees can access sites needed for work; and also apply a finer level of control and inspection for ransomware hosted within known and trusted domains such as social networking sites and other services.

- Cloud and/or premises-based web security gateway to protect all users, regardless of location
- Scalable to accommodate from 100 to more than 10,000 users
- Web security, application control, management, and reporting fully integrated
- Powered by Talos Threat Intelligence for comprehensive zero-day threat protection

Outbreak intelligence runs webpage components in a highly secure virtual emulation to determine how each component behaves and blocks any malware or ransomware.

The file reputation feature captures a fingerprint of each file as it traverses an organization's network. These fingerprints are sent to AMP's cloud based intelligence network for a reputation verdict. After an attack, using file retrospection, you can track a file's disposition over time after it enters your environment. If it is found to be malware, you can discover where the file entered and where it is currently located to mitigate future intrusions. Additionally, Cisco's Cognitive Threat Analytics (CTA) integrated feature helps reduce threat identification time by actively identifying the symptoms of a malware infection through behavioral analysis, anomaly detection, and machine learning.

Network monitoring

Cisco Stealthwatch provides visibility and security intelligence across an entire organization before, during, and after an attack. It continuously monitors the network and provides real-time threat detection and incident response forensics if a ransomware outbreak occurs.

Stealthwatch turns the network into a sensor, ingesting and analyzing NetFlow data from infrastructure and workstations, creating a baseline of the normal communication of an organization and its users. From this baseline, it is then much easier to identify when sophisticated attackers infiltrate the network trying to analyze and deploy ransomware. It can identify malware, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), and insider threats. It monitors both north-south and east-west (lateral) movements to detect the widest range of attacks.

Stealthwatch works in tandem with the Cisco Identity Services Engine (ISE) and Cisco TrustSec technology. Through this integration you can identify users and systems and appropriately segment critical network assets based on system behavior upon manual quarantine.

Identity-based segmentation

To best defend against the spread of ransomware, users should be allowed access only to the resources and system file shares they need to perform their duties. A system infected with ransomware will try to search the network for other file share drives and vulnerable systems to encrypt or infect them using the credentials of the current system user. It has become critical to identify the ransomware and segment the infected device before it spreads throughout the network.

Cisco TrustSec with Cisco ISE segments the network and enforces role-based access control. With Cisco TrustSec technology, you can control access to network segments and resources based on context, user, device, and location according to a specific security policy.

With Security Group Tags (SGT) enforcement, an infected user system with maintenance contractor credentials is blocked from accessing finance data, regardless of network topology or whether this contractor was using wired or wireless access to the network.

Through integration with Stealthwatch, if an infected system is identified based on abnormal behavior on the network, Cisco ISE can institute a change of authorization based on this learned behavior and apply a different SGT policy to quarantine it and immediately protect the rest of the network.

Infrastructure segmentation and intrusion prevention

Segmentation with NGFW

The Cisco Firepower Next-Generation Firewall (NGFW) is a fully integrated, threat-focused next-gen firewall with unified management. It delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint, each providing additional or alternate layers of defense against the threat of ransomware. Each of these capabilities working in concert serve to thwart network reconnaissance when your organization is targeted for a ransomware attack. Blocking communication between various network resources serves to segment your infrastructure to the permitted users, systems and protocols needed for business communications, and blocks those used to infiltrate, exploit, exfiltrate data, or retrieve encryption keys as well as to persist in your network.

Firepower NGFW enables comprehensive policy management that controls access, stops attacks, defends against malware, and provides integrated tools to track, contain, and recover from attacks that do get through.

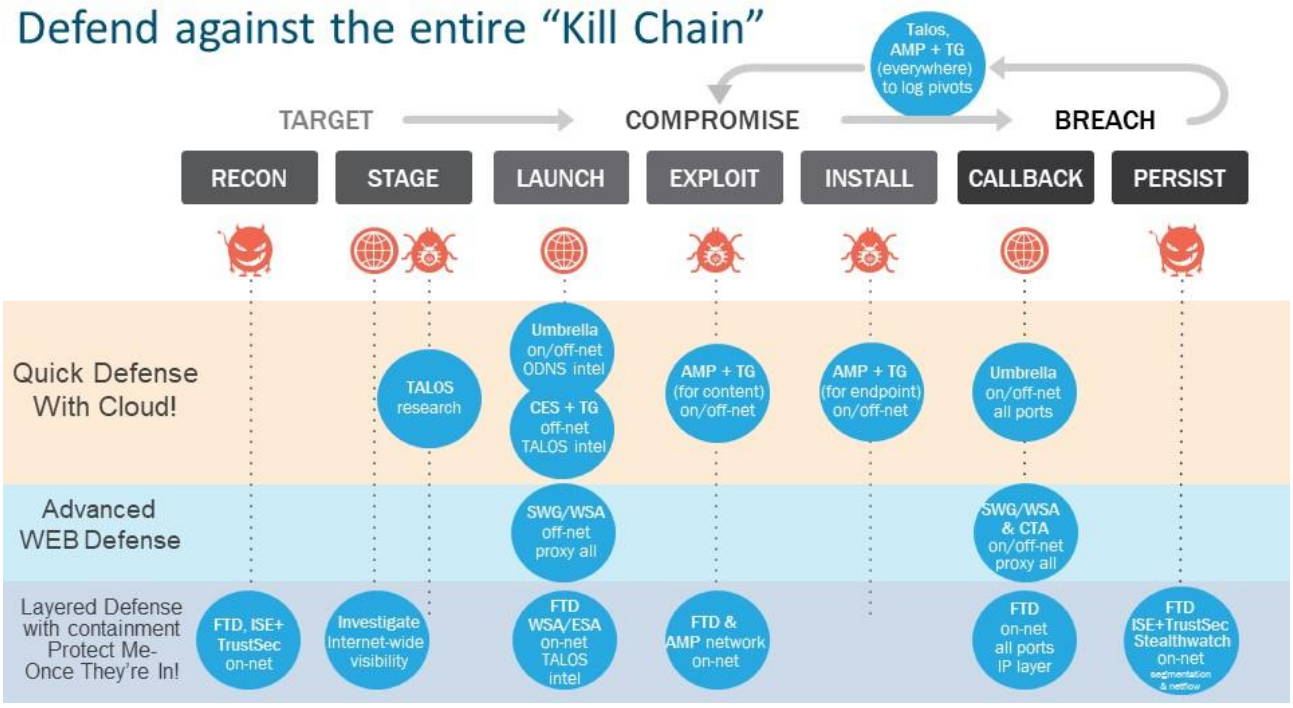
Management with Firepower Management Center

This is your administrative nerve center for network security management. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection on the Firepower platforms. It enables easy transitions from managing a firewall to controlling applications to investigating and remediating ransomware outbreaks. With the Cisco Firepower Management Center and Stealthwatch behavior analysis, you can share security intelligence and automate threat containment through ISE.

Architecture summary

Each of the products identified in the phases above fulfil the capability requirements necessary to defend against an attack across the kill chain, as shown in Figure 15.

Figure 15 – Product capabilities in the kill chain



Implementation Phase 1—Quick Prevention

The products listed in Table 3 were implemented for the Phase 1 validation testing of the Ransomware Defense Solution. Each of the product sections describes how they were customized after a typical installation to best defend against ransomware.

Table 3 - Solution products validated

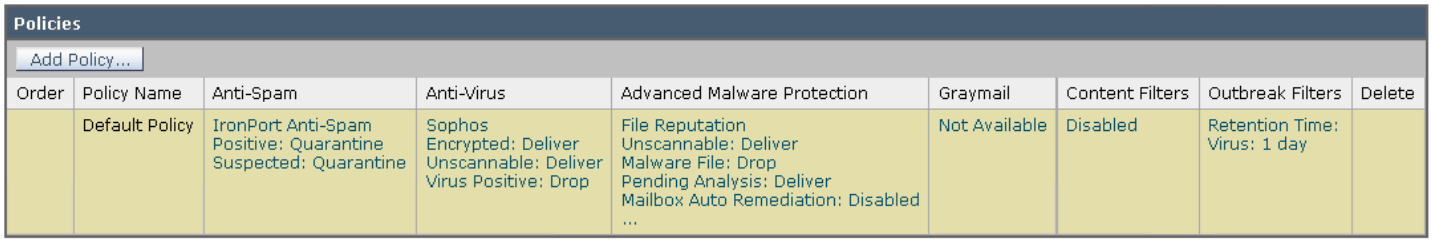
Product	Description	Platform	Version
Cloud Email Security	Email security with AMP	Cloud	v10.0.0-071
Umbrella roaming and network-based DNS protection	DNS security for roaming users outside the organization. Network DNS for all internal devices and systems	Cloud / Roaming client	v2.0.189
Advanced Malware Protection (AMP)	Host anti-malware protection for endpoints	Cloud / Client endpoint	v4.4.2.10200

Cisco Cloud Email Security

The following steps outline how to configure email security to best defend against ransomware and other advanced persistent threats (APT) after the Cloud Email Security service is up and functioning normally and fully integrated into your mail process flows. For a new CES installation, the Default Policy should be similar to Figure 16.

Step 1 Select **Mail Policies > Incoming Mail Policies**.

Figure 16 - Default policy for new deployment



Within the Incoming Mail Policies, we edit the Default Policy elements of Advanced Malware Protection, Content Filters, and Outbreak Filters.

Advanced Malware Protection

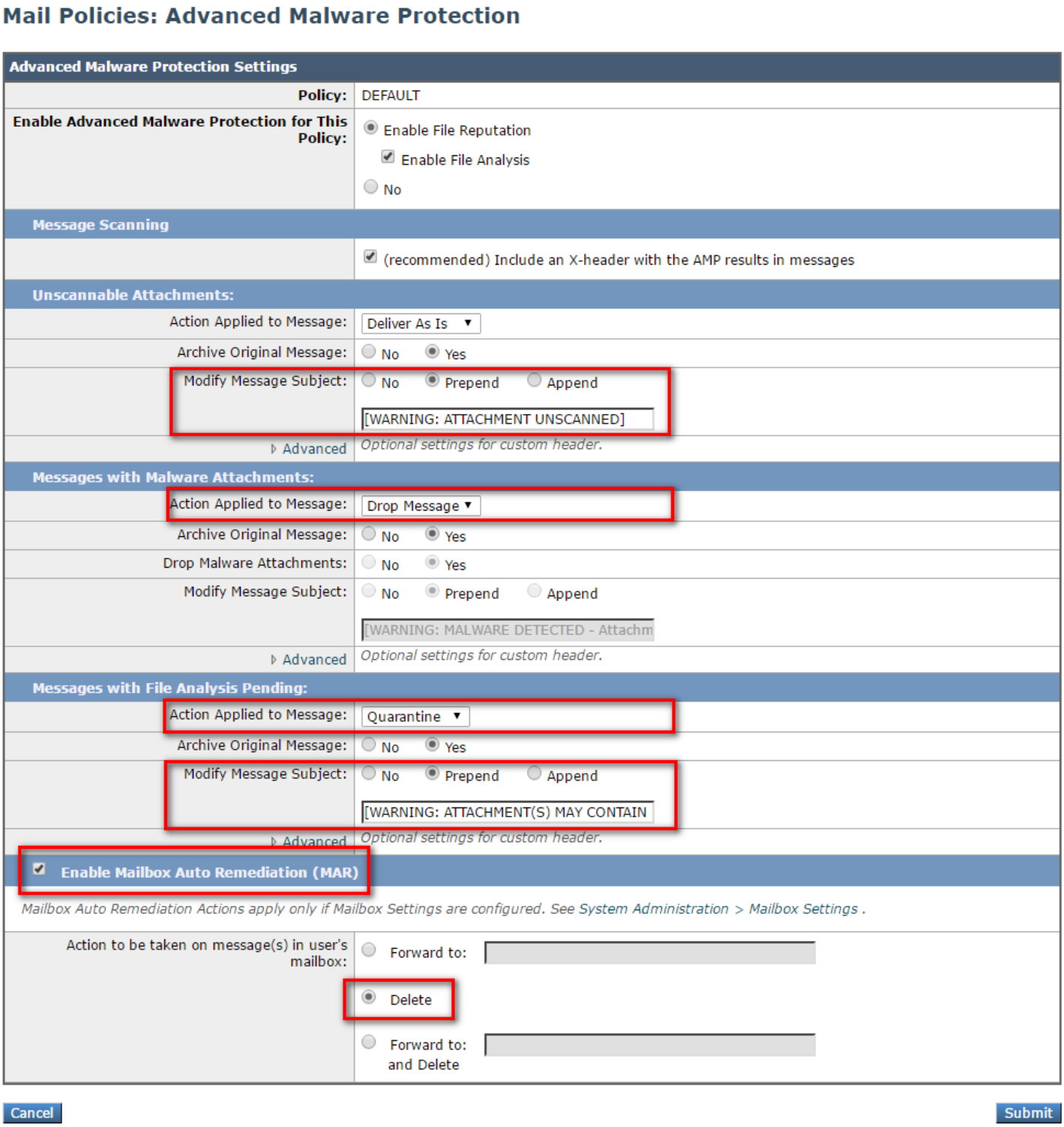
Next, configure the Incoming Mail Policy for File Reputation Scanning and File Analysis using Advanced Malware Protection. Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:

- Obtaining the reputation of known files
- Analyzing behavior of certain files that are not yet known to the reputation service
- Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network

These features are available only for incoming messages. Files attached to outgoing messages are not evaluated.

Step 2 Click the link in the Advanced Malware Protection column of the Default Policy to modify it.

Figure 17 - Advanced Malware Protection in default policy



It is a best practice to prepend the email message subject with an informative warning based on the status of the messages attachments.

Step 3 Configure the Modified Message Subject for both Unscannable Attachments and File Analysis Pending results.

Messages with malware attachments may have the attachments stripped, delivered with a warning, or dropped altogether. The most common practice is to drop the entire message.

Step 4 Configure the **Action Applied to Message > Drop Message.**

Messages with File Analysis Pending can be either delivered or quarantined. The best practice is to quarantine these email messages until a result is received by the analysis engine. If the attachment is malicious, it follows the Attachments setting. If the result returned is unknown, the message is delivered and the Message Subject prepended with a warning.

Step 5 Configure the **Action Applied to Message > Quarantine.**

By enabling Mailbox Auto Remediation (MAR), messages already delivered to a user's mailbox can be deleted when the threat verdict later changes to malicious.

Step 6 Configure MAR by checking **Enable**, and set the action to **Delete**.

Step 7 When finished with these changes, click **Submit**.

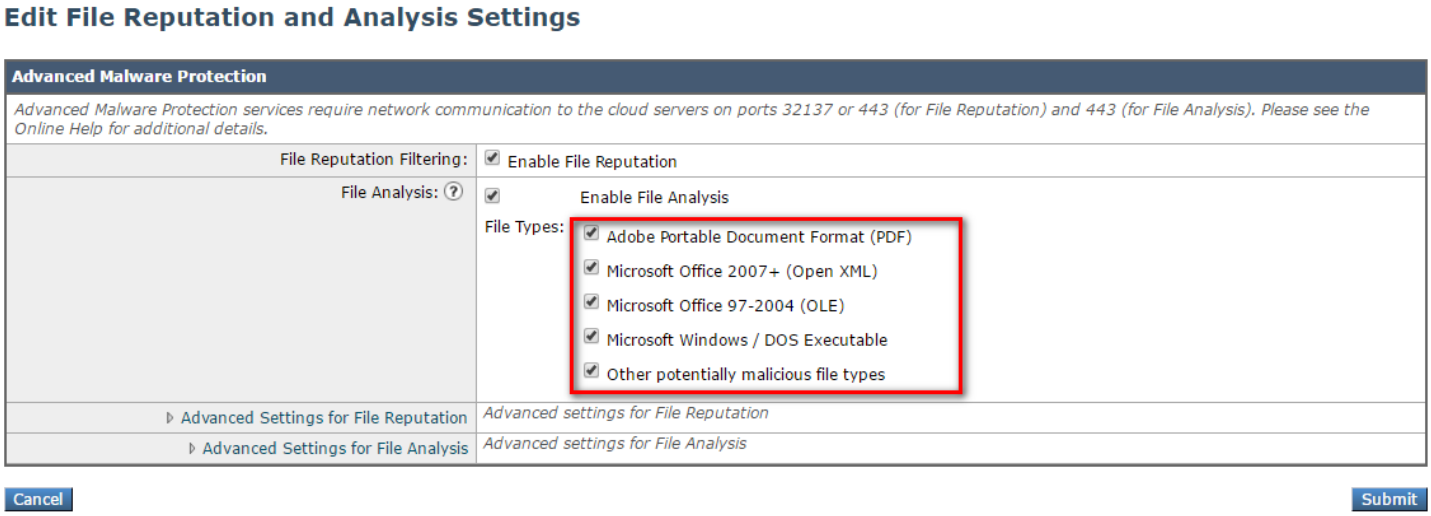
File Reputation and Analysis Service implements the AMP engine for inspecting messages as enabled by the policy above. File Analysis is enabled by default for new implementations and inspects Windows and DOS executables, but you should also select additional file types for analysis.

Step 8 Select **Security Services > File Reputation and Analysis.**

Step 9 Select **Edit Global Settings.**

Step 10 Enable additional file types, as shown in Figure 18. Click **Submit**.

Figure 18 - File Analysis settings



Content Filtering

Some ransomware and exploit kits are attached to messages as scripts. These are not inspected by file analysis yet, and these scripts can run locally on the system if opened and bypass security in web browsers. As a best practice, Cisco recommends using content filtering to remove these types of script attachments: .js or .wsf or .vbs

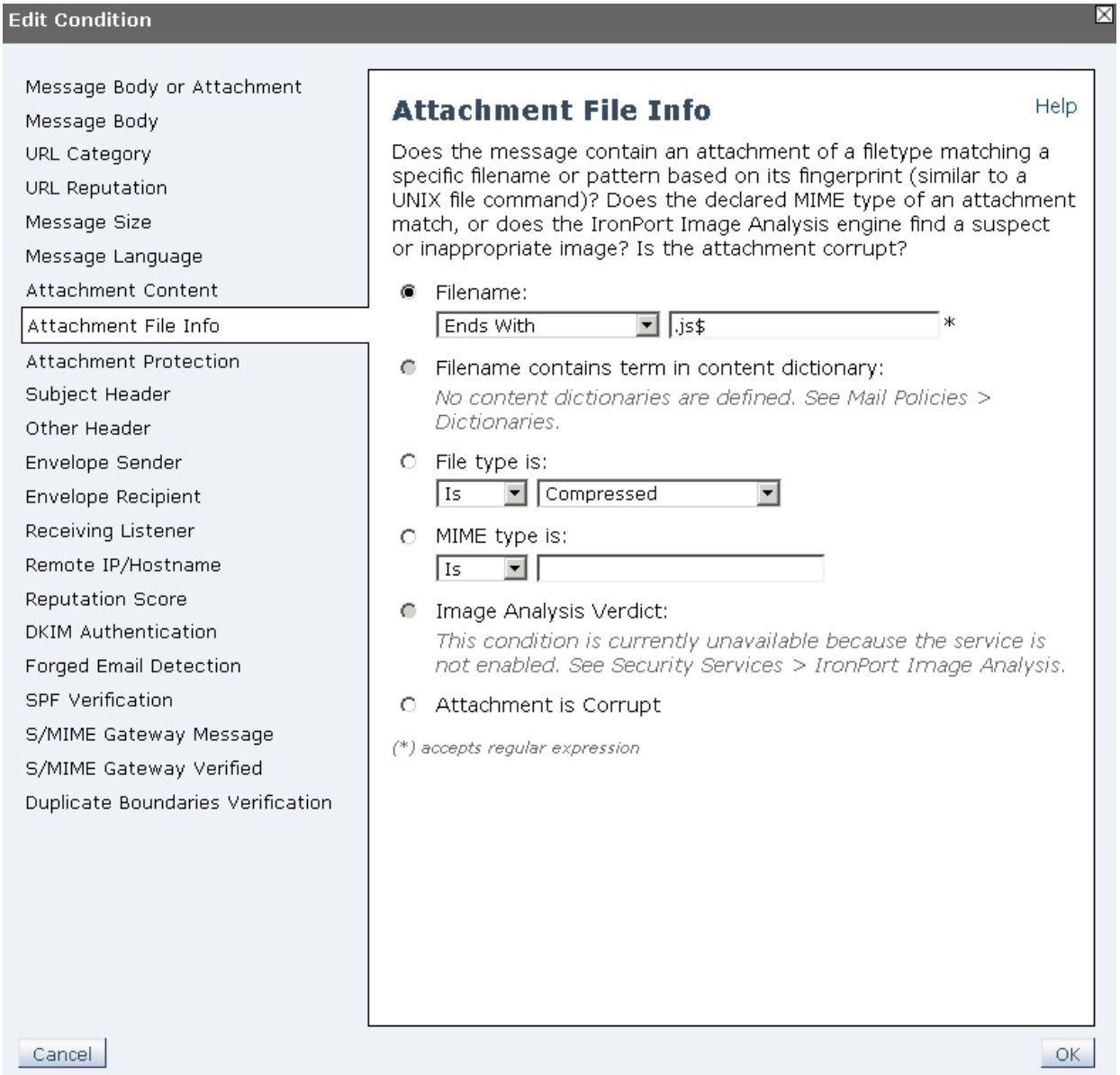
Create a new incoming content filter to drop messages with these attachments.

Step 11 Select **Mail Policies > Incoming Content Filters >Add Filter**.

Step 12 Give it a descriptive name and description.
Name: BlockScriptAttachments
Description: Save people from Ransomware by blocking script attachments: .js or .wsf or .vbs

Step 13 Click **Add Condition > Attachment File Info > Filename Ends With .js**.

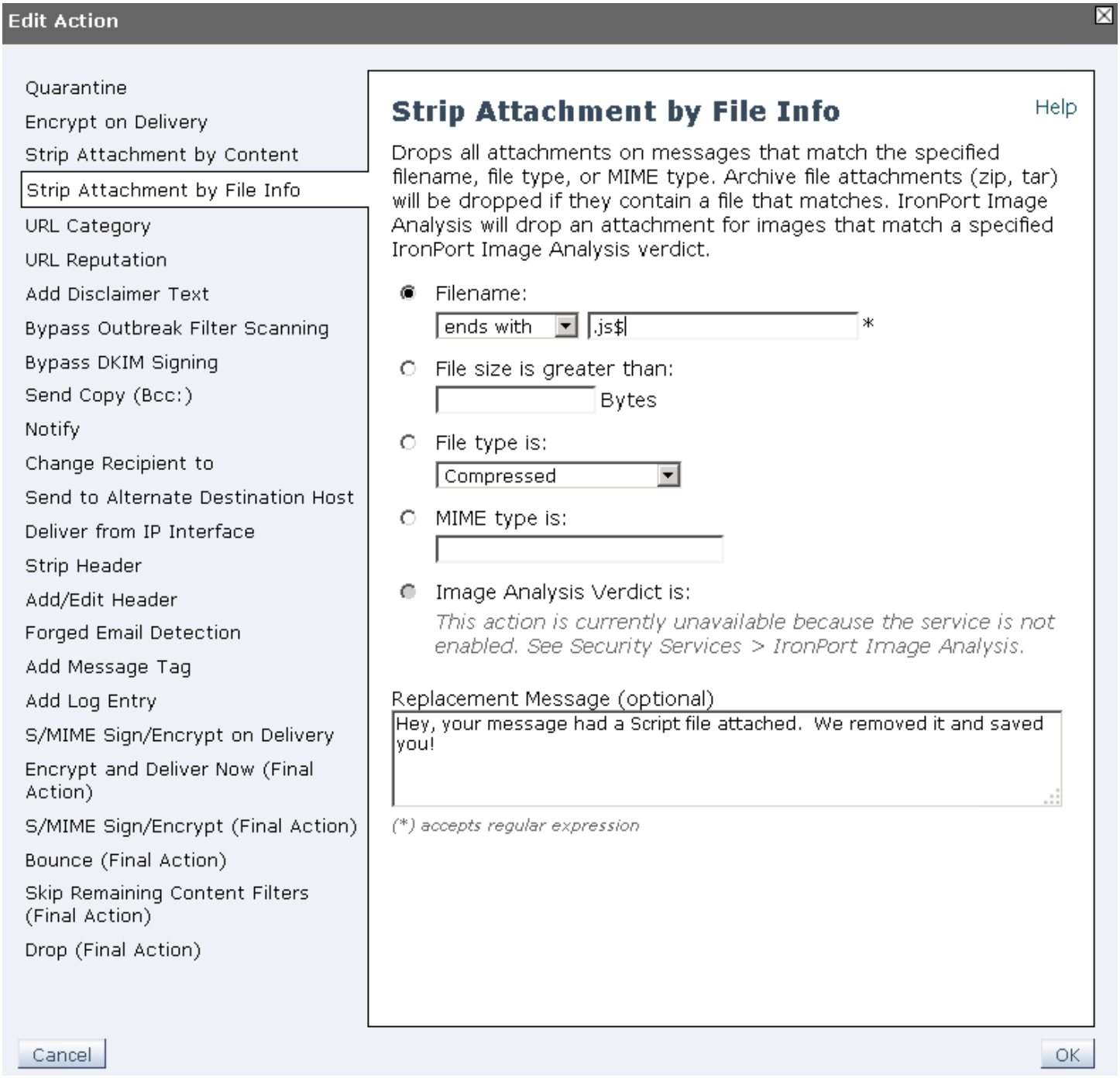
Figure 19 - New content filter condition



Step 14 Click **OK**.

Step 15 Click **Add Action > Strip Attachment by File Info > Filename ends with .js$**.

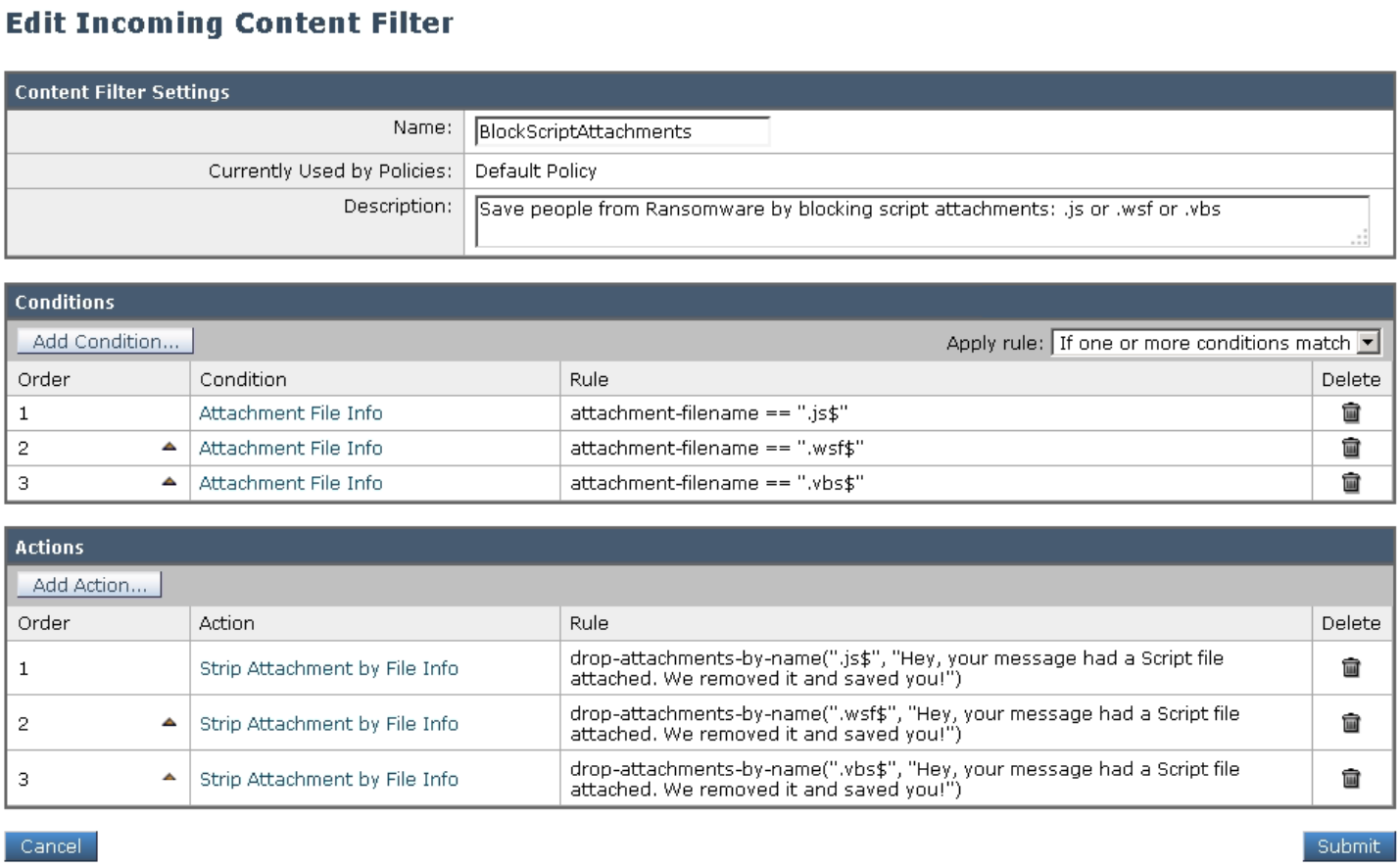
Figure 20 - New content filter action



Step 16 Click **OK**.

Repeat Steps 13-16 for .wsf and .vbs file types as well. Your final filter should include all six, as shown in Figure 21.

Figure 21 - Content filter that removes script files



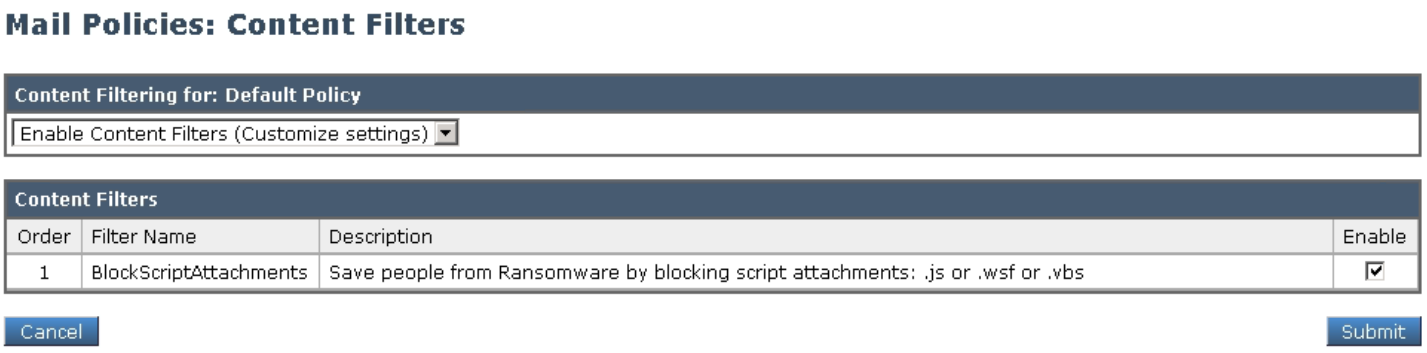
Step 17 Click **Submit** when finished.

Enable the new Content Filter in the Default Policy

Step 18 Select **Mail Policies > Incoming Mail Policies > Disabled** in the Content Filter column of the Default Policy to modify it.

Step 19 Select **Enable Content Filters** in the dropdown, check the Enable column for the newly created filter.

Figure 22 - Enable content filtering and filter



Step 20 Click **Submit** when finished.

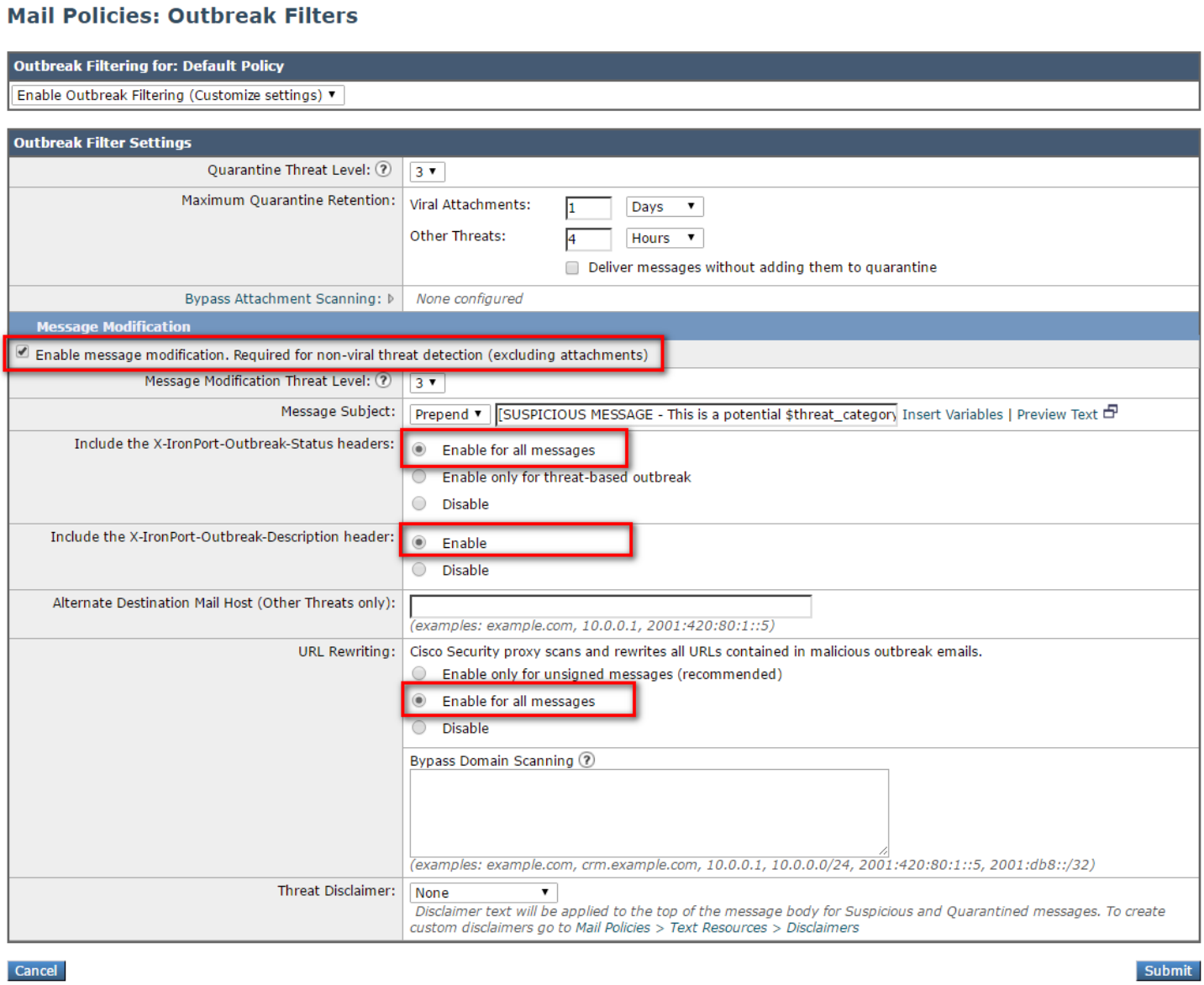
Outbreak filters

Outbreak filters protect your network from large scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur. Cisco gathers data on outbreaks as they spread and updates the threat intelligence services in real-time to prevent these messages from reaching your users.

For new installations, the Outbreak Filter is enabled by default, but it is a best practice to also enable message modification, which enables URL rewriting on messages. This feature informs users to use caution when opening specific messages.

Step 21 Select **Mail Policies > Incoming Mail Policies > Retention Time** in the Outbreak Filter column of the Default Policy to modify it.

Figure 23 - Outbreak filter message notification



Step 22 When finished enabling message modification, click **Submit**.

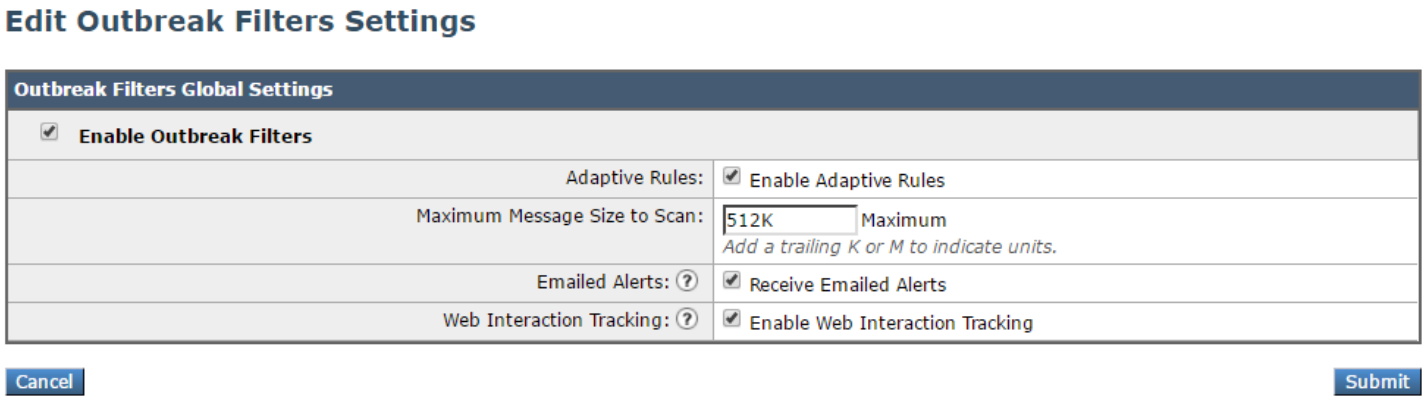
Web Interaction Tracking

Web Interaction Tracking allows administrators to track the end users who click on URLs rewritten by Cisco Email Security. This allows tracking of messages with malicious links, including who clicked on the link and the results of their actions.

By default, Web Interaction Tracking is disabled. To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking.

Step 23 Select **Security Services > Outbreak Filters > Edit Global Settings**.

Figure 24 - Web Interaction Tracking for outbreaks

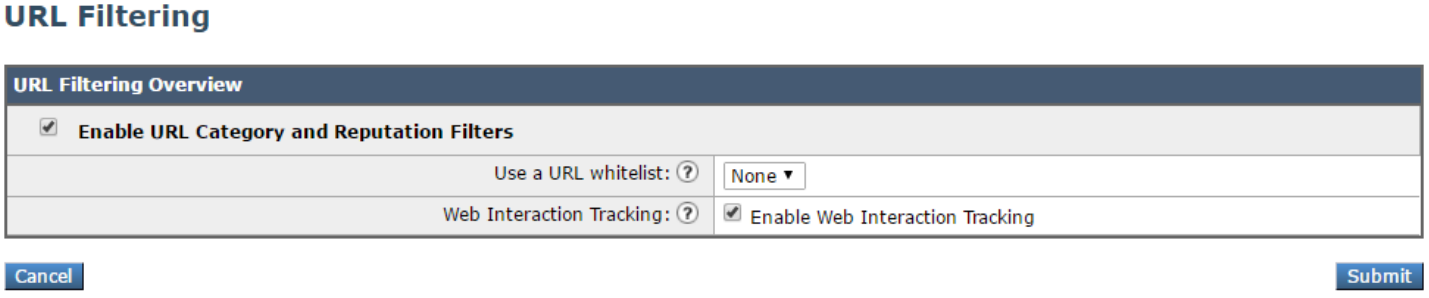


Step 24 Check the **Email Alerts** and **Web Interaction Tracking** checkboxes. Then click **Submit**.

To also track URLs due to policy rewrites, you must also enable Web Interaction Tracking in the URL filtering settings.

Step 25 Select **Security Services > URL Filtering > Enable**.

Figure 25 - Web Interaction Tracking for URL filter



Step 26 Click **Enable URL Category and Reputation Filters** checkbox, and **Web Interaction Tracking**. Then click **Submit**.

When finished with all changes, you need to commit the changes for these new settings to take effect.

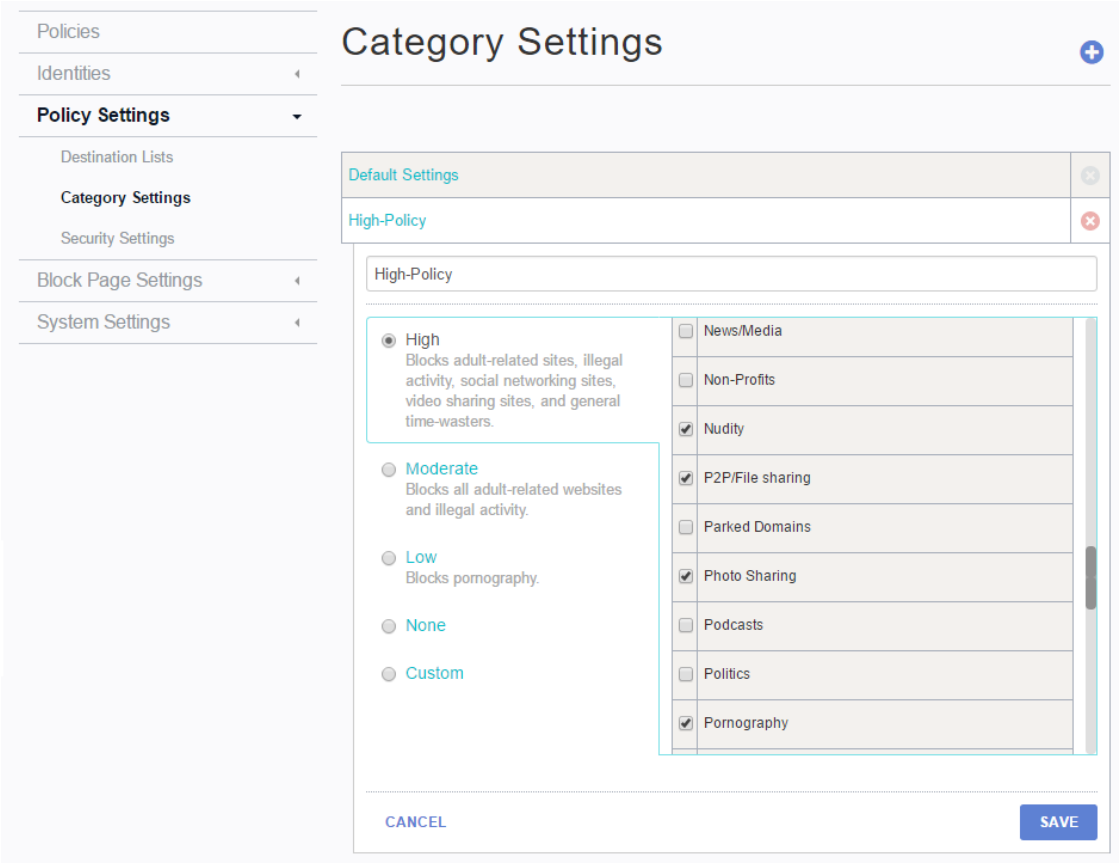
Step 27 Click the yellow Commit Changes button in the upper right corner, leave an appropriate comment, then click **Commit Changes** to submit them.

Cisco Umbrella DNS security

Cisco Umbrella

The complete Cisco Umbrella offering can protect network, roaming, and mobile devices. It includes a more comprehensive set of policy options, including restricting access to other categories of content, which may also reduce the risk of being directed to domains were ransomware may be hosted (e.g., Gambling, P2P/File sharing, Hate/Discrimination). Several pre-configured policies are available in addition to creating a custom policy. Figure 26 shows the High policy that was used in our validation testing.

Figure 26- Umbrella High policy

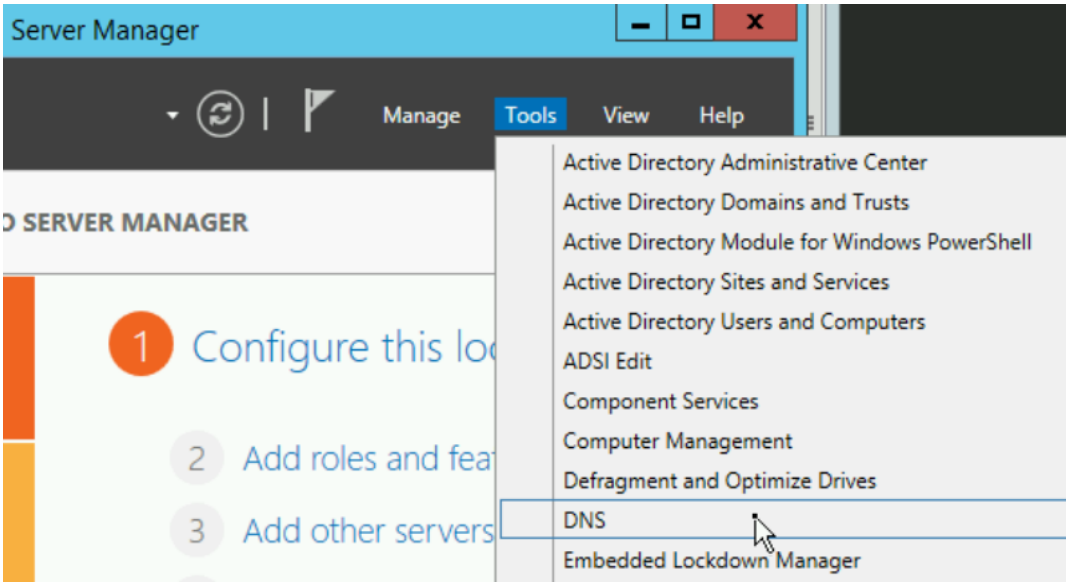


For organizations that implement their own internal network DNS servers, Umbrella can be easily enabled for the entire network. Configure your DNS server to use the Umbrella servers as forwarders instead of performing their own root lookups for external domains. This eliminates the need to deploy the Umbrella client on any internal network system, making for a simple clientless implementation that protects everything on the network.

The following steps outline how to configure Windows DNS forwarding to use Umbrella as we did for part of our validation testing.

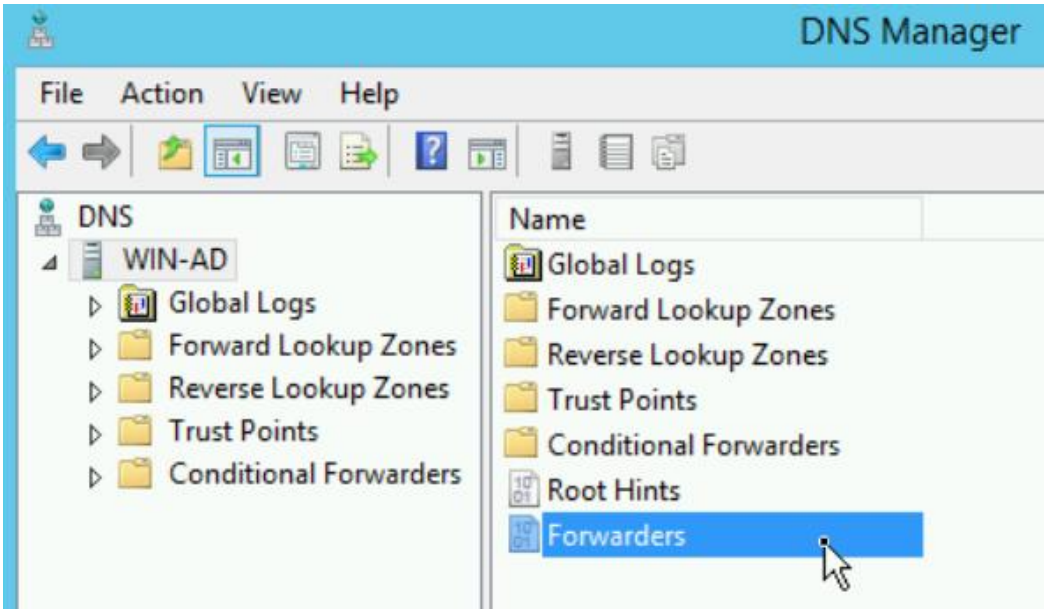
Step 1 Open Windows DNS manager under Server Tools.

Figure 27 - Windows DNS Manager



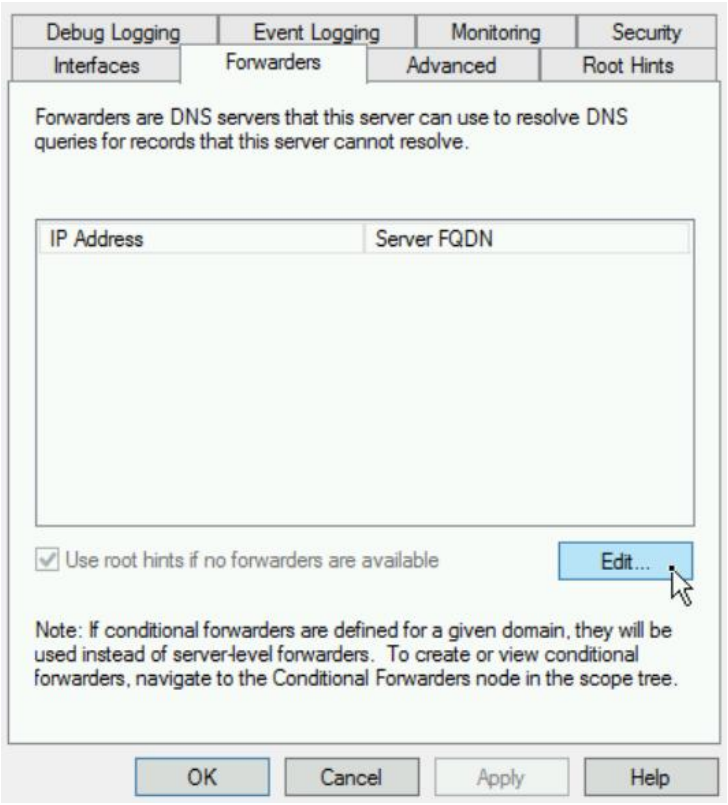
Step 2 Choose the server to edit, then select **Forwarders**.

Figure 28 - Windows DNS manage—Forwarders



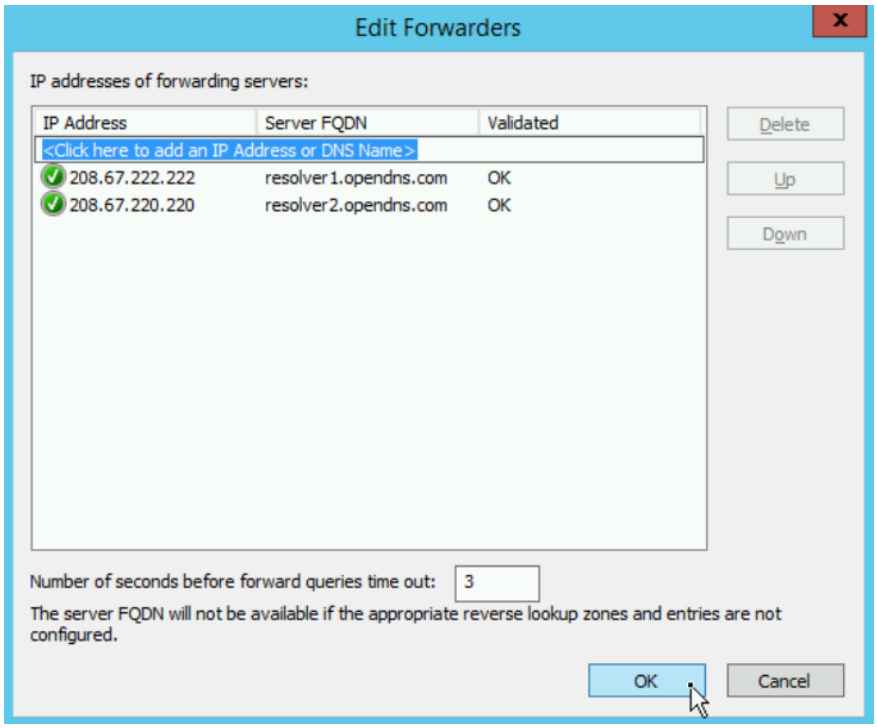
Step 3 Click **Edit**.

Figure 29 - Edit Windows DNS—Forwarders



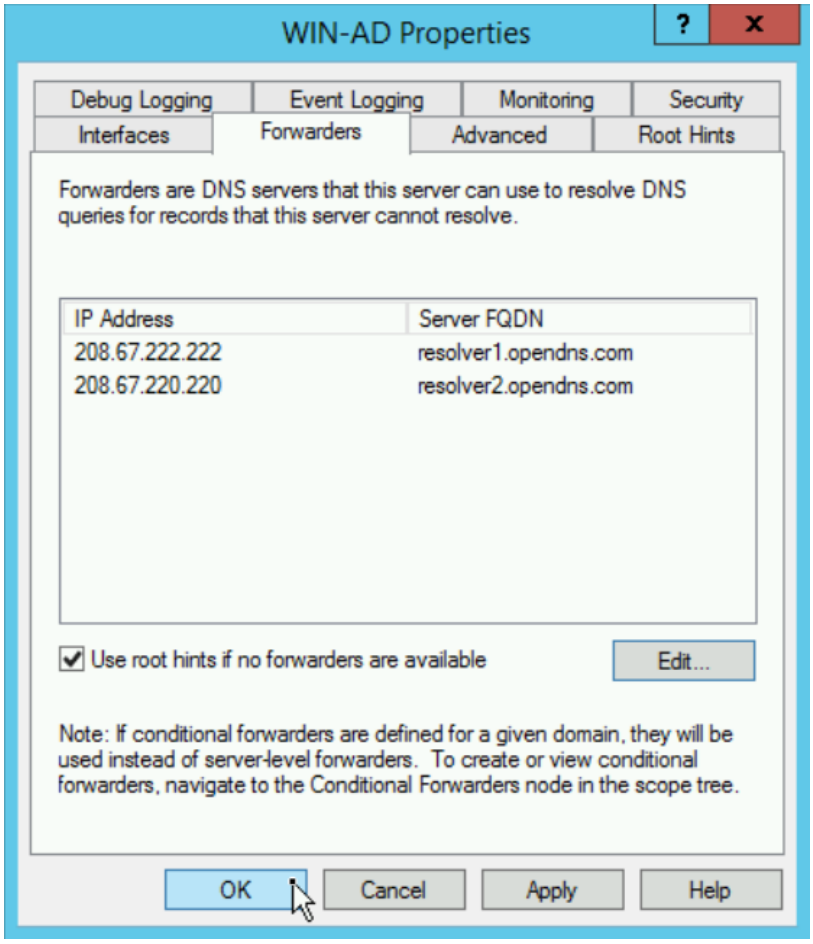
Step 4 Enter the addresses for the Umbrella DNS servers; 208.67.220.220, 208.67.222.222; and then click **OK**.

Figure 30 - Add Windows DNS forwarders



Step 5 Click **OK** to commit the changes and close the configuration window.

Figure 31 - Complete changes to Windows DNS Manager



Next, add the public IP address that your DNS server uses to the network identities in Umbrella.

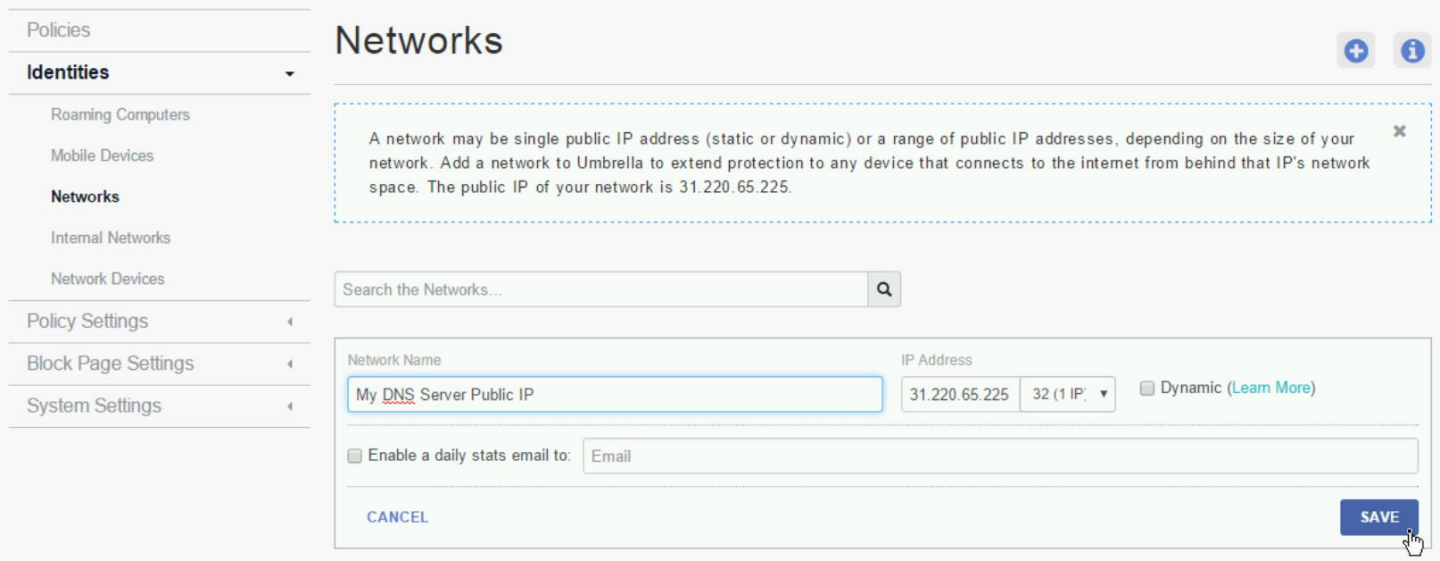
Step 6 Select **Configuration > Identities > Networks**.

Step 7 Click the “plus” icon to add a new network.

Figure 32 - Add Umbrella DNS network

Step 8 Enter the public IP address of the network along with the subnet mask, usually a /32 subnet. and choose a descriptive name. Then click **Save**.

Figure 33 - Configure new network

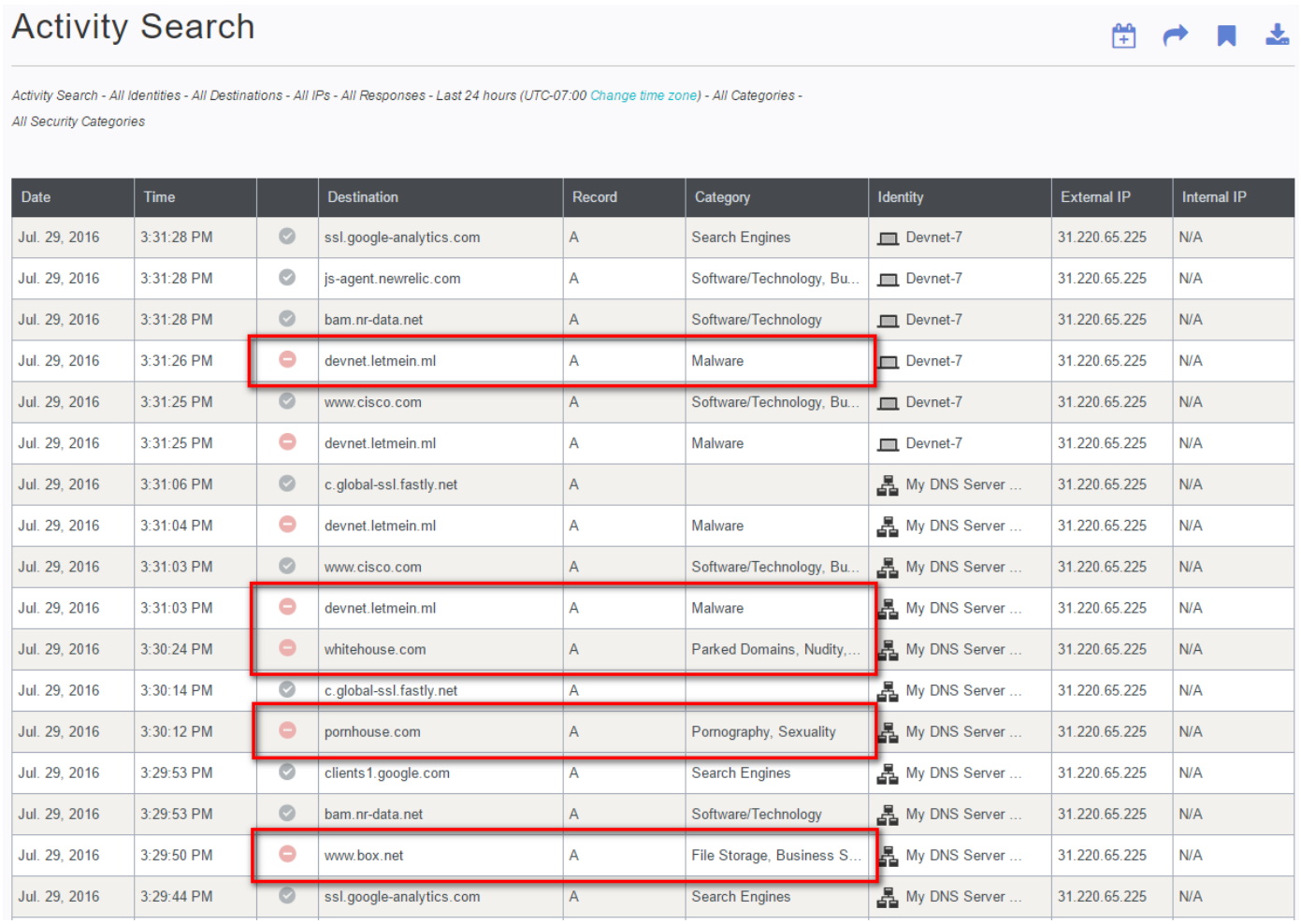


Now all systems that use the internal network DNS server are protected, and all activity reporting can be attributed to requests from the internal DNS server.

The Activity report shows all DNS lookup actions, and clearly designates what destination domains were blocked and the category to which that destination belonged.

Figure 34 shows the results of the blocked domain when trying to download ransomware or access other category-blocked sites. Identity information includes the Umbrella Roaming Client system and lookups from the internal DNS server.

Figure 34- Umbrella blocked domain lookups



Activity Search

Activity Search - All Identities - All Destinations - All IPs - All Responses - Last 24 hours (UTC-07:00 Change time zone) - All Categories - All Security Categories

Date	Time		Destination	Record	Category	Identity	External IP	Internal IP
Jul. 29, 2016	3:31:28 PM		ssl.google-analytics.com	A	Search Engines	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM		js-agent.newrelic.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM		bam.nr-data.net	A	Software/Technology	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:26 PM		devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM		www.cisco.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM		devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:06 PM		c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:04 PM		devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM		www.cisco.com	A	Software/Technology, Bu...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM		devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:24 PM		whitehouse.com	A	Parked Domains, Nudity,...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:14 PM		c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:12 PM		pornhouse.com	A	Pornography, Sexuality	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM		clients1.google.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM		bam.nr-data.net	A	Software/Technology	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:50 PM		www.box.net	A	File Storage, Business S...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:44 PM		ssl.google-analytics.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A

Cisco Umbrella Roaming Client

The Umbrella Roaming Client serves to protect laptops regardless of where they are in the world or how they connect to the Internet. The client works by securely redirecting DNS queries bound for the Internet to the Umbrella Secure Cloud Gateway via one of the OpenDNS Global Network data centers distributed worldwide, so that your policies are enforced as you choose and security is applied, preventing your computers from becoming compromised.

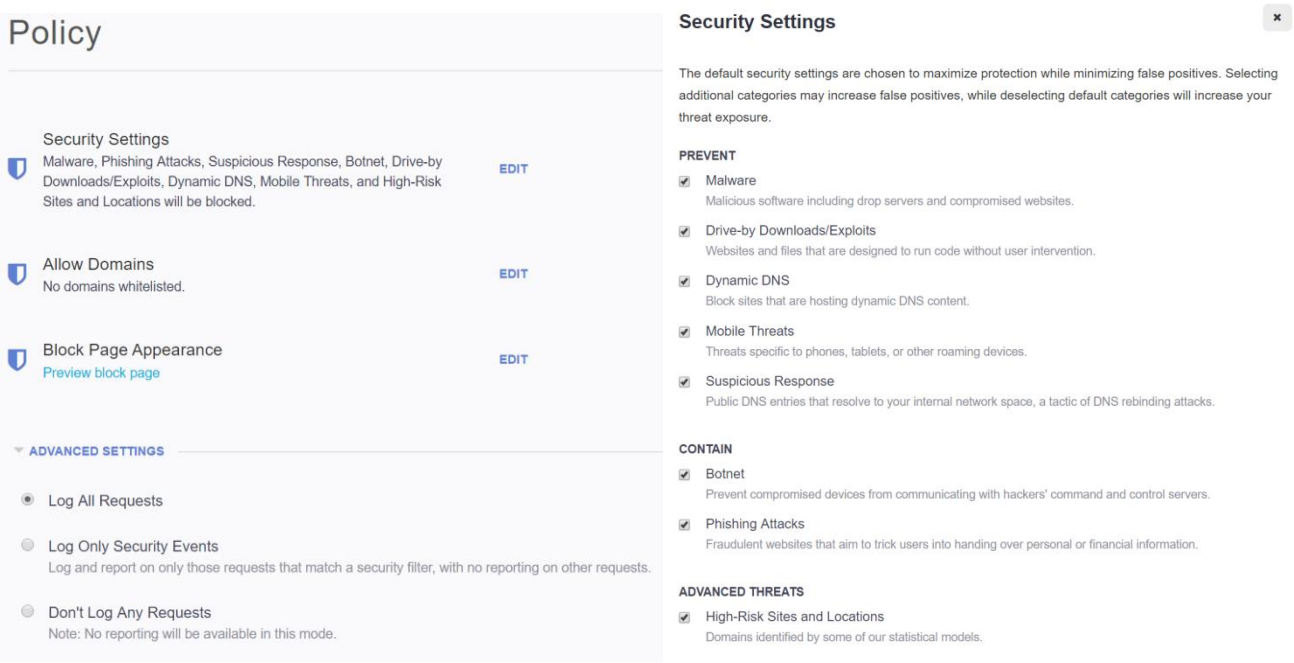
Several scenarios include computers accessing the Internet through 3G/4G wireless carrier networks, untrusted networks via Wi-Fi hotspots (e.g., airport, café, hotel, home), and within office environments behind trusted network gateways or Umbrella-protected networks.

There are no additional configuration steps needed to defend against ransomware. The procedure for downloading and installing the roaming clients can be found here: http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf

Cisco Umbrella Roaming

The Cisco Umbrella Roaming only offering uses a simplified policy that blocks critical security threats, as shown in Figure 35.

Figure 35- Cisco Umbrella Roaming Computers Policy



Cisco Advanced Malware Protection for Endpoints (AMP)

AMP is a cloud-based “software-as-a-service” solution. Once your account is set up, you configure a policy and then deploy AMP’s lightweight connector on your endpoints. Supported endpoints include connectors for Windows, Mac, Linux, and Android systems. If your organization has high-privacy restrictions, an alternative deployment option includes an on-premises, air-gapped AMP Private Cloud Virtual Appliance, which is outside the scope of this solution validation.

The first time you log into the FireAMP console, you are presented with the first-use wizard. This wizard can walk you through some of the steps to quickly configure your FireAMP environment by creating exclusions for antivirus products, setting up proxies, configuring a policy, and creating groups. These steps are covered in the QuickStart Guide[3] and not duplicated here.

The following additional configuration steps are needed to provide the best protection possible against ransomware. Several settings are performed in the policy used by your system groups, others in the AMP account settings. First, edit the policy settings: enable Execute Mode, which blocks files from being run until they have been scanned; and increase the maximum scan and archive file size limits as appropriate to fit your organization. Of the 1600+ ransomware samples we collected for solution validation, 103 of them were larger than the default 5MB Maximum Scan File Size in the Protect Policy (the largest was 51MB).

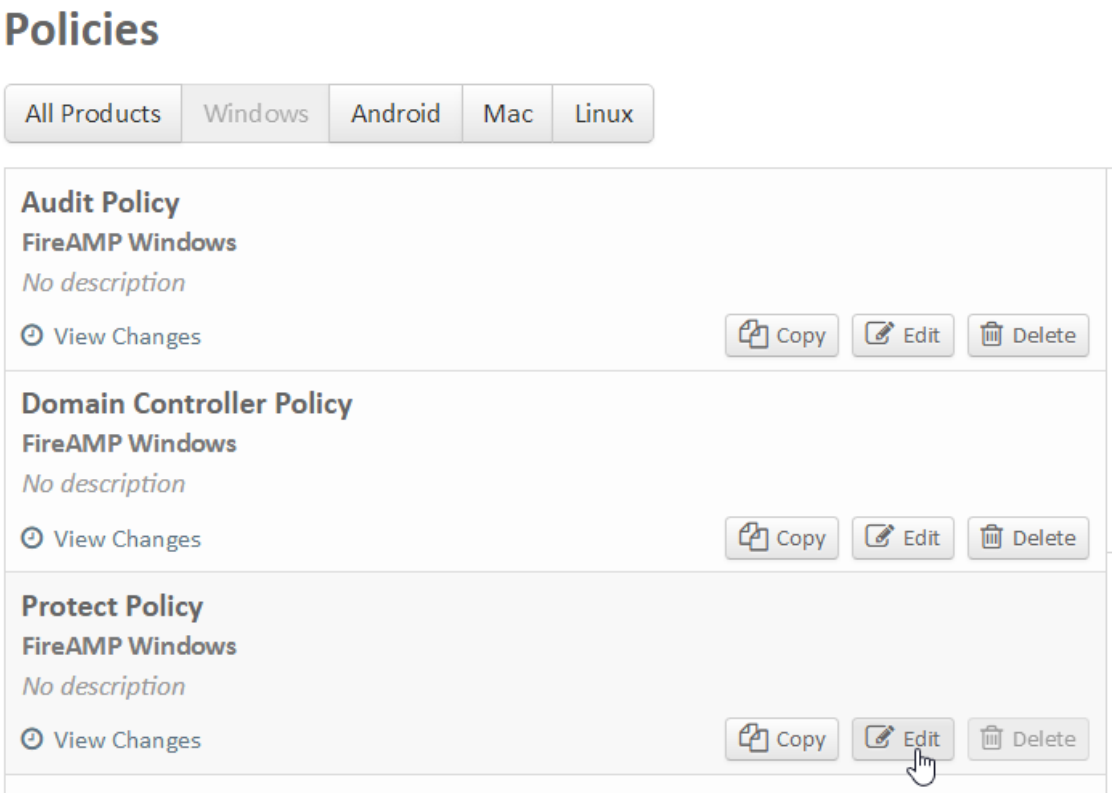
NOTE: Larger file sizes for scanning increase WAN utilization to the Internet, and may affect other communications. For large organizations, an onsite scanning appliance may be a preferred option.

[3] https://docs.amp.cisco.com/FireAMPQuickStartGuide.pdf

Step 1 After logging in to the AMP Console, select **Management > Policies**.

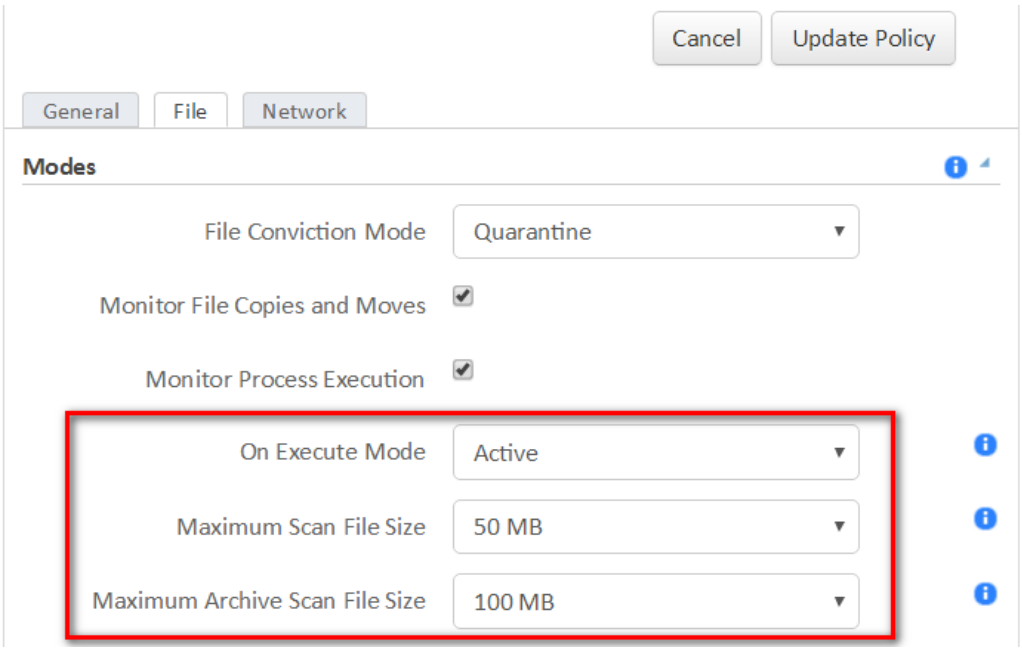
Step 2 Select the appropriate Protect Policy you are deploying to your endpoints and click **Edit**.

Figure 36 - AMP Protect Policy



Step 3 Change to the File tab of the policy, set On Execute Mode to **Active**, and set max file sizes.

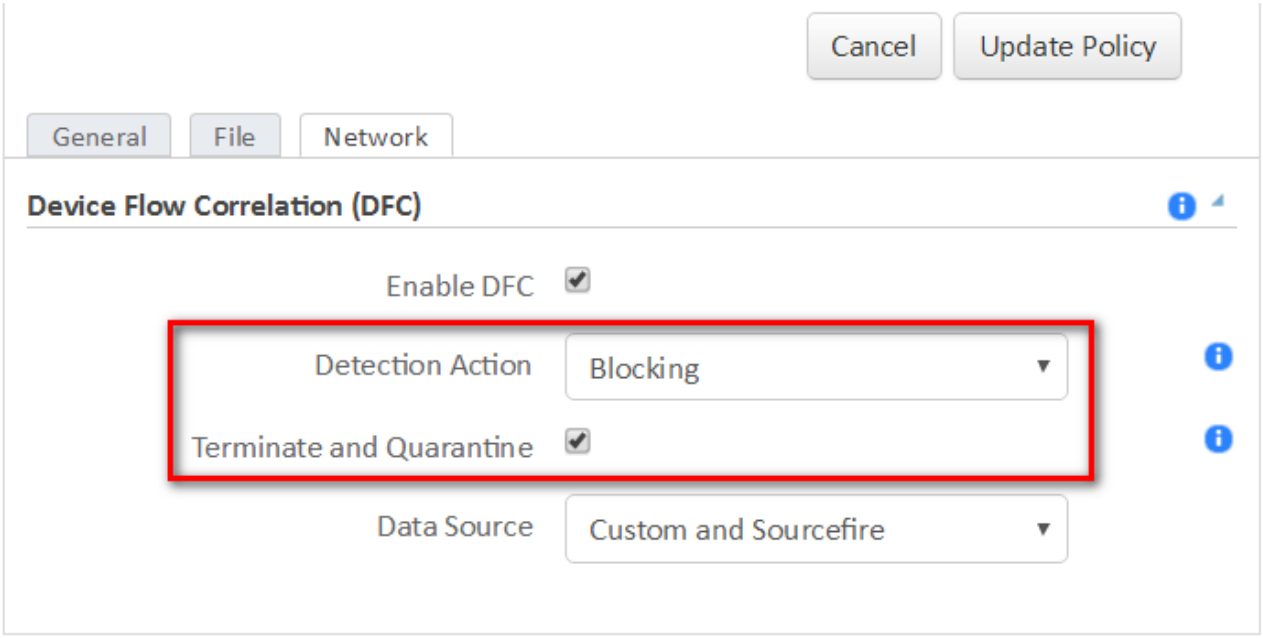
Figure 37 - Edit Policy file attributes



Device Flow Correlation (DFC) can stop ransomware callback communications at the source, and is especially useful for remote endpoints outside the corporate network.

Step 4 Select the **Network** tab, set DFC Action to **Blocking**, Check **Terminate and Quarantine**.

Figure 38 - Edit Policy network attributes



WARNING! Before enabling this feature, make sure you have whitelisted any applications allowed in your environment, particularly any proprietary or custom software.

Step 5 Click **Update Policy** when finished.

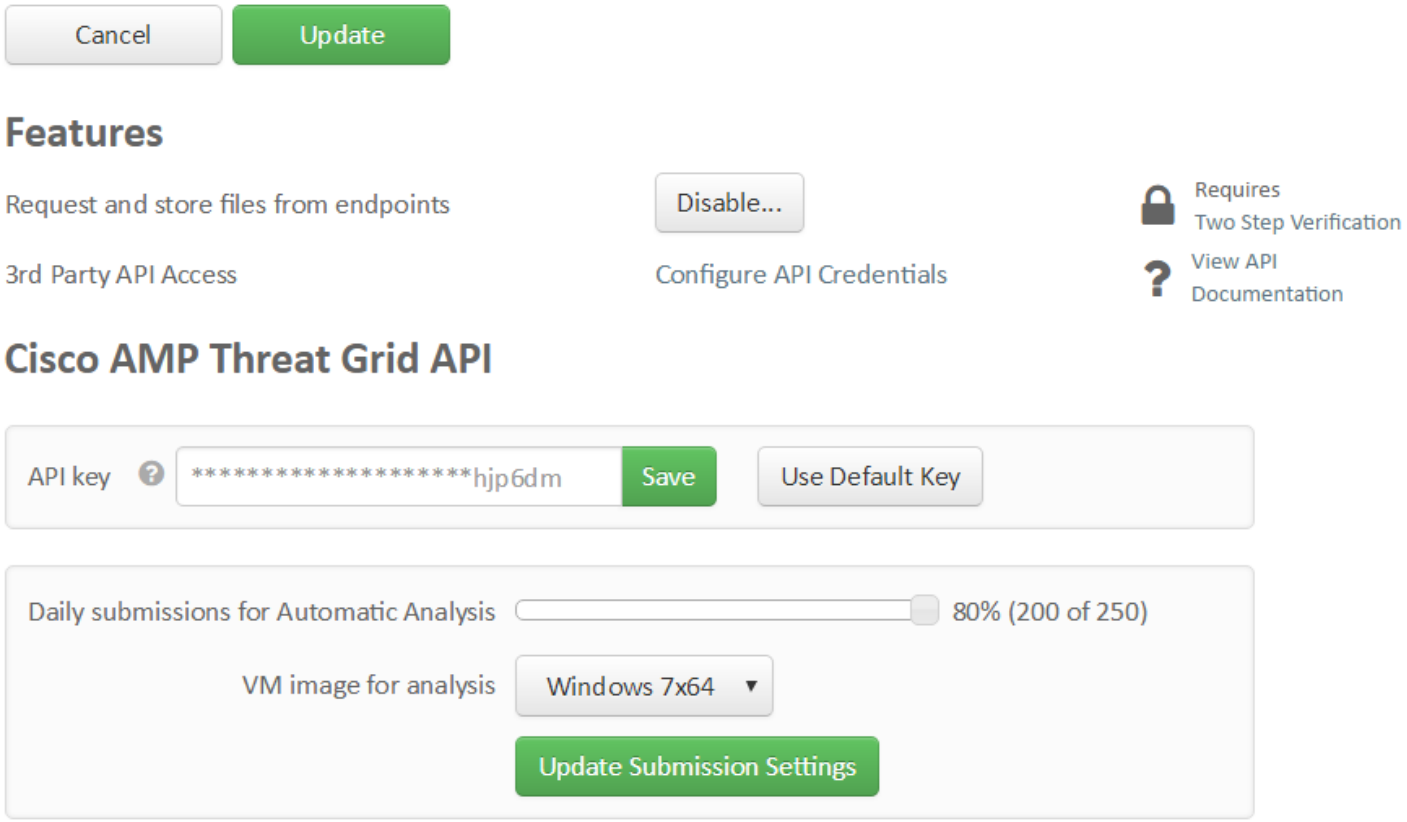
The Cisco AMP Threat Grid API allows you to automatically submit files for analysis. Before configuring Auto analysis, all users must have two-factor authentication enabled for their accounts to ensure that the highest level of privacy is maintained as all analyzed files are accessible by the administrative users configured in the console.

Once two-step verification is enabled on your accounts, you can then edit the accounts business settings to enable the file repository, API key, and submission settings.

Step 6 Select **Accounts > Business > Edit**.

Step 7 Under Features, enable **Request and store files from endpoints**, set your Threat Grid API key if you have a separate account, slide the “Daily submissions for Automatic Analysis” to the desired level, and select the VM image that best matches the majority of your endpoints. Click **Update Submission Settings**.

Figure 39 - AMP account business settings



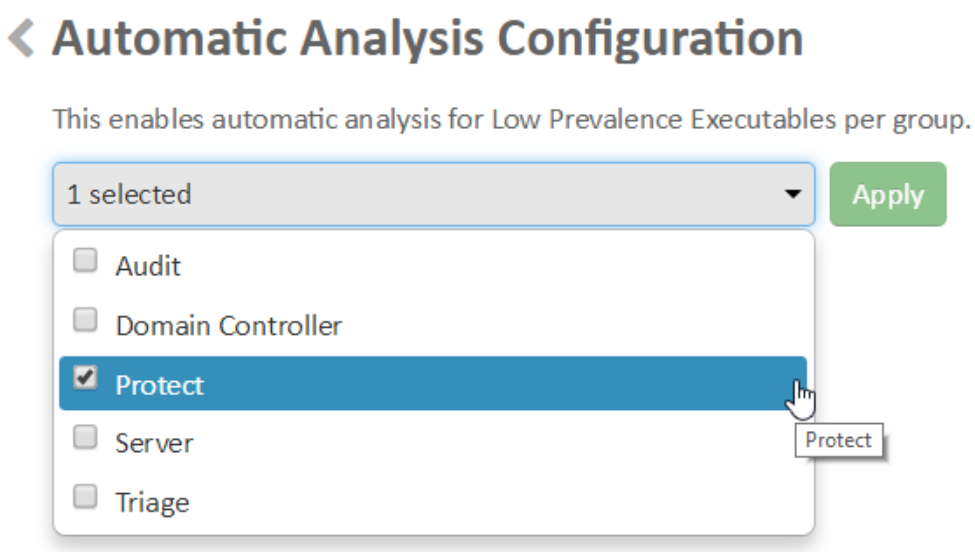
Step 8 When finished, click **Update** at the top to update your account settings.

Now enable automatic analysis to send low prevalence executable files from specific groups to file analysis.

Step 9 Select **Analysis > Prevalence > Configure Automatic Analysis**.

Step 10 Select the system groups for which you want to enable Automatic Analysis and click **Apply**.

Figure 40 - Enable AMP Automatic Analysis



Once you have configured Automatic Analysis, low prevalence executable files are submitted every four hours. FireAMP requests the file from the FireAMP Connector that observed it if it is available. Once the file has been retrieved, it is submitted to File Analysis. You can then view the results of the analysis from the File Analysis page. If the file is not retrieved for a period of time, you can check the file fetch status in the File Repository.

Implementation Phase 2 advance solution

The products listed in Table 4 were implemented for the validation testing of the Ransomware Advanced Defense Solution. Each of the product sections describes how they were customized after a typical installation to best defend against ransomware.

Table 4 - Solution products validated

Product	Description	Platform	Version
Stealthwatch	Collect and analyze NetFlow	Virtual or appliance	6.9.0
ISE	Authenticate and profile devices connecting to network	Virtual or appliance	2.2.0.470
Cognitive Threat Analytics	Analysis of flows from SW	Cloud	No versions
Firepower Management Center	Manage Firepower Threat Defense systems	Virtual or appliance	6.2.0
Firepower Threat Defense	Security platforms running Firepower Threat Defense software image	Virtual and 2100, 4100, 9300	6.2.0
ASA	Firewall	ASA5500-X	9.7(1)4
ASA-ASDM	Local FW Mgmt	ASA5500-X	7.7(1)
NGIPS on ASA	Protection and control	ASA5500-X	5.4.1.8+
AnyConnect	Secure Mobility Client	All	4.4.02039
Catalyst Switches	Aggregation	6880 6807-XL	15.2(1)S 15.4(1)SY
	Access	3650, 3850	16.3.3

Cisco Identity Services Engine (ISE)

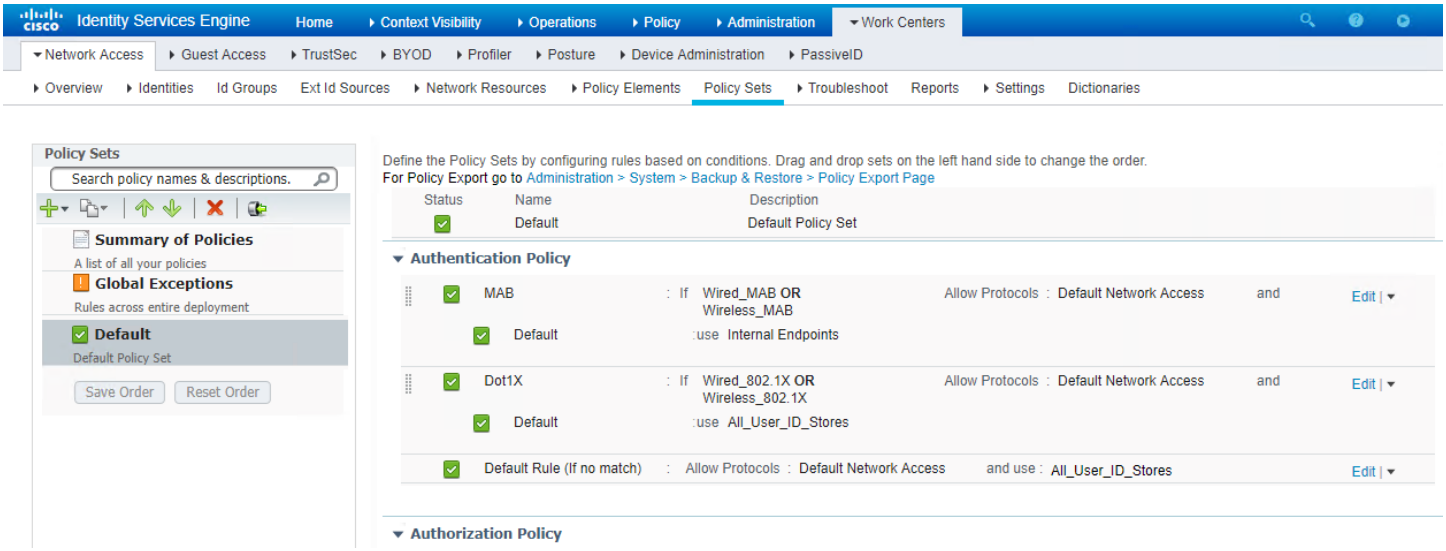
Authenticating people and devices as they connect to the network infrastructure is the first line of defense for protecting the company. It is the opportunity to segment known from unknown, and trusted from untrusted. This contextual information can then be used throughout the company in many other policy enforcement areas as well as tying identity to the visibility of communication flows.

This guide focuses on the configuration of the ISE against ransomware, and at a high level, Users. Information on how to deploy ISE, and alternate configurations can be found here: https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html

Configuring network authentication

It is crucial for the network administrators to identify the devices onboarding into the network regardless of the different vectors users will access. Whether they are accessing via wired, wireless, or even though a VPN connection, their security policy needs to be effective. In this environment, through the AAA authentication, we set the security tagging by ISE.

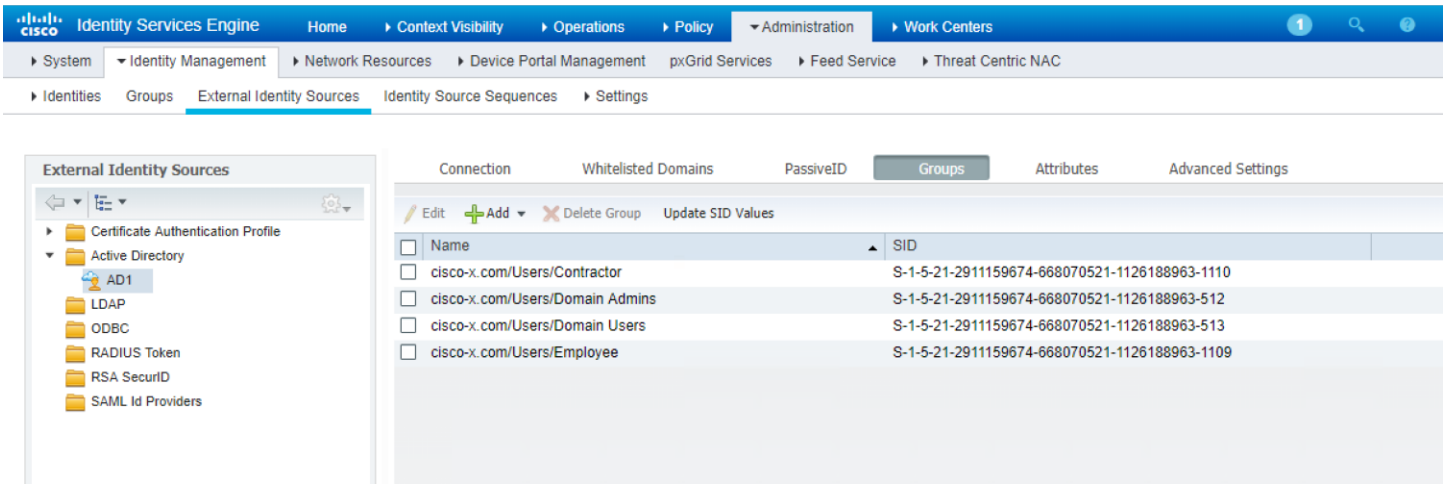
Figure 41 - Default policy set



The default authentication policy for ISE first looks at a device's MAC address and tries to match it to a known manufacturer to pass the authentication phase. The administrator can also configure Dot1X as an authentication method to identify the users or devices.

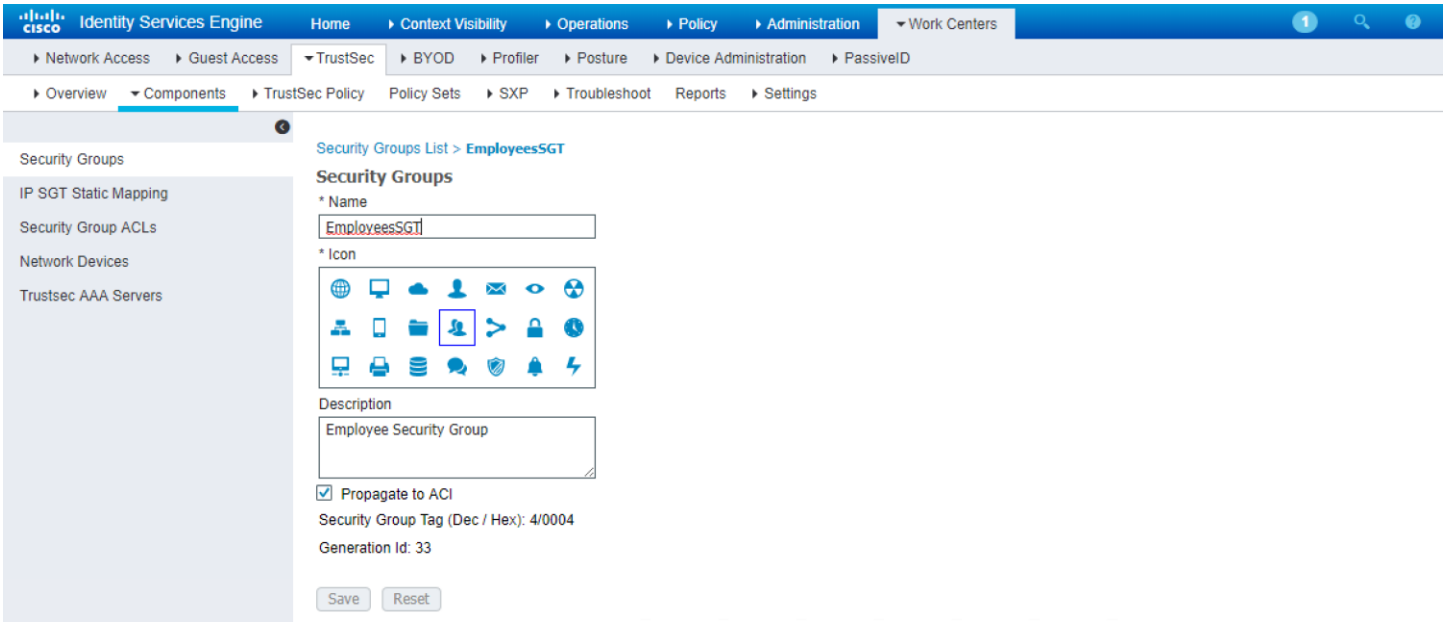
In this example, we created two groups: Employee and Contractor. These values are associated with an Active Directory's group name. Upon setting Active Directory, these values can be downloaded into ISE as a group. They are also found in Administration > Identity Management > External Identity Sources > Groups.

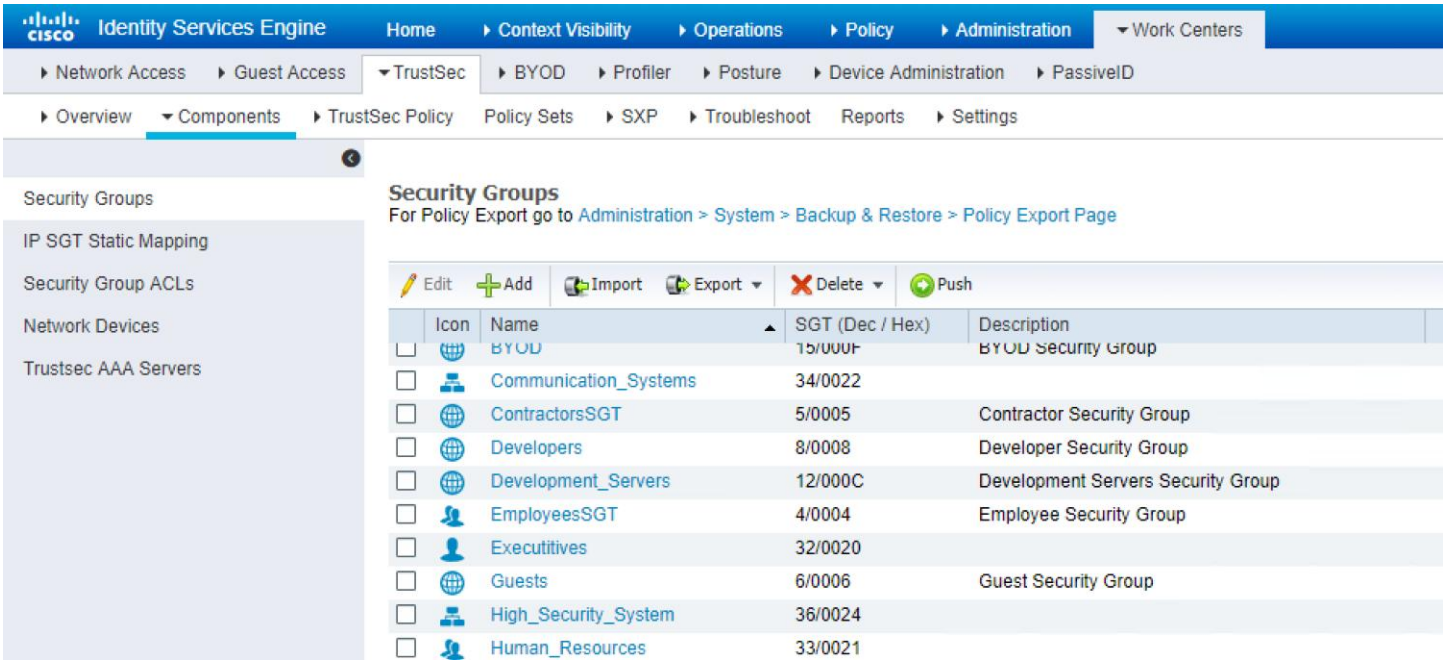
Figure 42 – External identity sources



Step 1 After you have configured ISE to recognize the Active Directory group, create TrustSec Security Group Tagging (SGT). In this example, we created EmployeeSTG and ContractorSTG. Note: An SGT ID will be automatically generated as Employee: STGID 4 and Contractor: STGID 5

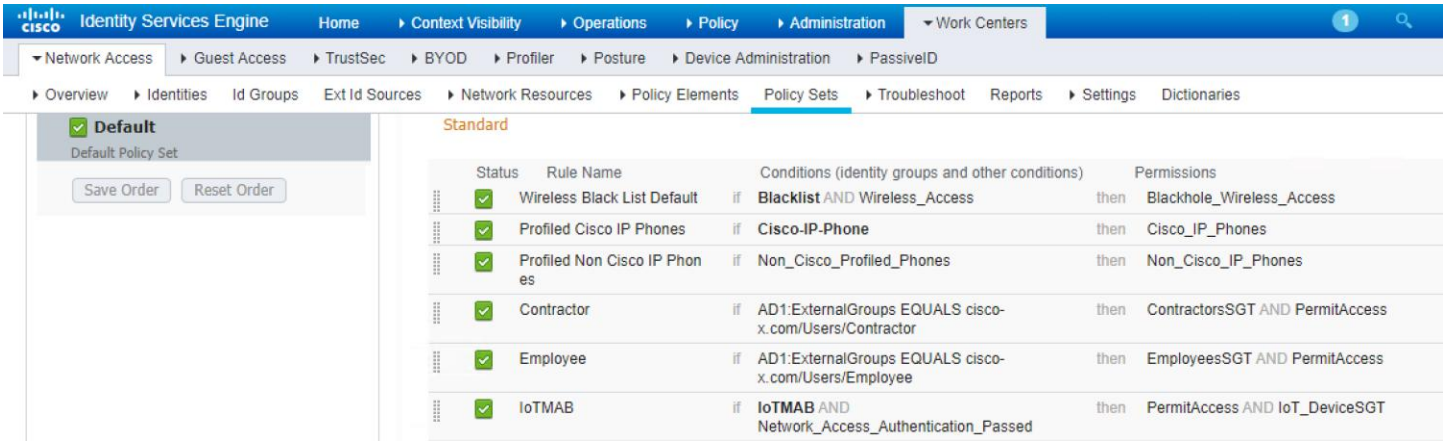
Figure 43 – TrustSec SGTs





Step 2 Create an authorization rule for Employee and Contractor and assign permissions and security group tags.

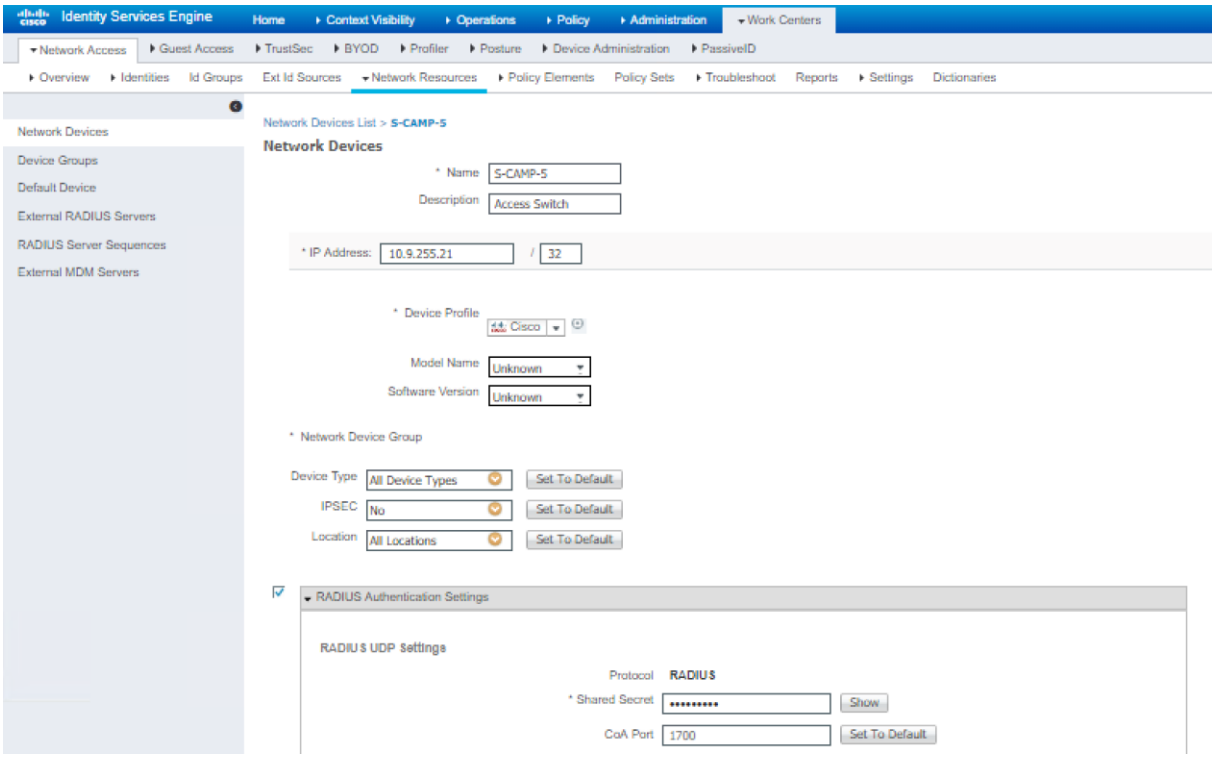
Figure 44 – Authorization rule



The condition of the rule is if the authentication matches the Active Directory server (AD1), and the authenticated user is part of the Employee or Contractor group, it assigns a corresponding SGT and permits access.

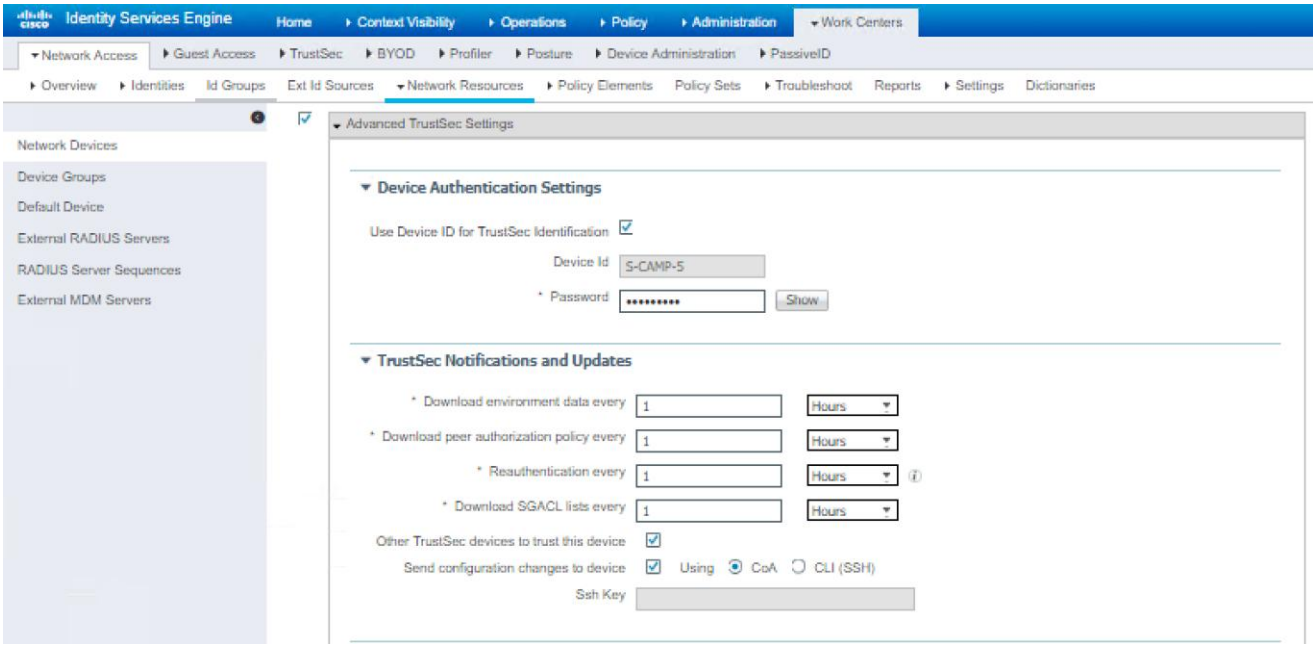
Step 3 Add switches, firewalls, and routers to ISE that will authenticate devices and users. Select **Work Centers > Network Access > Network Resources > Network Devices.** Click **Add**. Enter the name, IP address, and description (optional). Set the RADIUS shared secret.

Figure 45 – Add network devices



Step 4 Set the TrustSec device ID to use the device name. Set the password to be used for authentications. Click **Save**.

Figure 46 – Set TrustSec device ID



Switch configuration

Each switch must be configured to communicate with the ISE AAA server for authorizing network devices, users, and other systems. A best practice is to do this end-to-end across the company, enabling the most comprehensive view of what is connected to the network.

Configure RADIUS authentication, authorization, and accounting

Step 1 Globally specify the interface that has the IP address configured in ISE that will be used for authentication. Enable dot1x control. Enable AAA.

```
ip radius source-interface Loopback0
dot1x system-auth-control
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

Step 2 Configure the following RADIUS server attributes:

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
```

Step 3 Configure the RADIUS Server, IP address, and shared secret that was entered in ISE.

```
radius server ISE01
 address ipv4 10.9.10.51 auth-port 1812 acct-port 1813
 pac key Cisco1234
```

Step 4 Configure the AAA group name for RADIUS and specify the server created in Step 3.

```
aaa group server radius ISE
 server name ISE01
```

Step 5 Configure the default Authentication, Authorization, and Accounting to use the group created in Step 4.

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting update periodic 2880
aaa accounting dot1x default start-stop group ISE
```

Step 6 Enable ISE to automatically send policy updates to the switch when there is a Change of Authorization (CoA). Enter the password specified in the ISE device configuration for Advanced TrustSec settings. This facilitates a bounce, re-authentication, or disabling of a switch port.

```
aaa server radius dynamic-author
 client 10.9.10.51 server-key Cisco1234
```

Step 7 Set the device tracking command in the switch so it can send the IP address to the ISE. The command for device tracking may differ, depending on the type of switch and/or version is installed.

Prior to IOS 16.1.x, you may use

```
ip device tracking all
```

in the global configuration mode

After IOS 16.1.x,

Global command:

```
device-tracking tracking
!
device-tracking policy IPDT
 tracking enable
```

On the dot1x interface:

```
device-tracking attach-policy IPDT
```

For more information, please refer to: IOS 16.1.x configuration guide

NOTE: For switches with operationally critical systems, bounce and disable commands can be overridden and ignored with these configurations.

```
authentication command bounce-port ignore
authentication command disable-port ignore ip device tracking
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

Enable port authentication per port

On the switch, the following configurations enable port-based authentication and IP device tracking. Configure each interface that will have an endpoint device connected. For MAB and Dot1x methods to co-exist and function as expected, the order and priority must be properly specified as referenced in this application note: Configuring MAB http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html

Step 7 Add the following configurations to each device interface:

```
interface GigabitEthernet1/1
 device-tracking attach-policy IPDT
 authentication event fail retry 0 action next-method
 authentication host-mode multi-auth
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

The ***port-control auto*** command is what activates enforcement, and can be added or removed for testing.

TrustSec

Configuring TrustSec throughout the company involves several steps. The first step is to define the policies that specify which groups are allowed to communicate with each other. Policies that use these security groups are created separately in both ISE and firewall policy managers (Firepower Management Center, ASDM, CSM). After the desired policies are defined, each system is configured to share the SGT-to-IP address mappings information using Security Exchange Protocol (SXP). Some environments require in-line tagging of packets in addition to participation in SXP. Lastly, enforcement is enabled on switches and firewall interfaces.

The Cisco Platform Exchange Grid (pxGrid) provides a highly secure system for other technologies to exchange intelligence. Deploy pxGrid between ISE, Firepower and Stealthwatch to share rich contextual information of users and devices connected to the network. Steps to install pxGrid can be found in the Rapid Threat Containment Design guide.

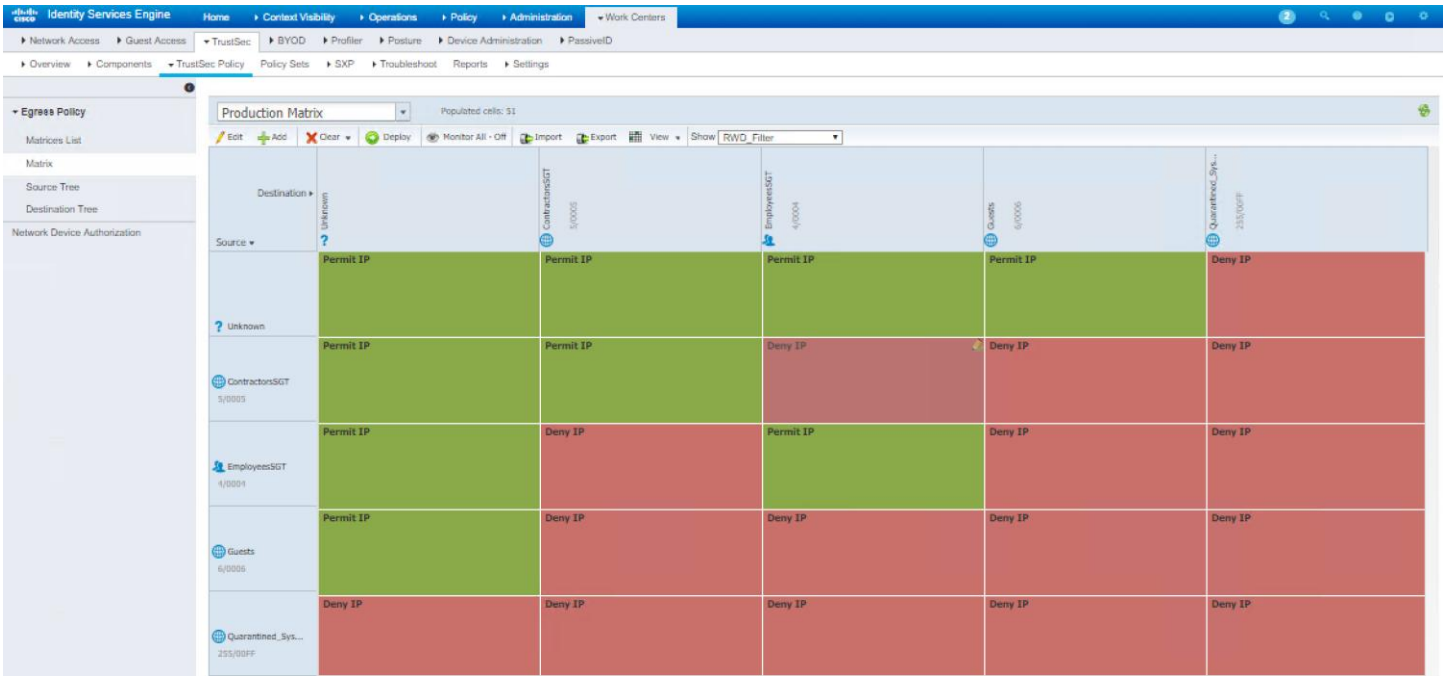
ISE policy matrix

The communications controlled by the ISE policy matrix and enforced by switches are unidirectional and not stateful, so consideration must include both requests and replies for proper symmetry and expected functionality. Enforcement happens when packets exit the access switch port with the destination device/security group attached.

ISE with TrustSec is ideal for implementing security at the switch level between devices on the same switch, within or between cells, and creates the desired segmentation throughout the Industrial zone.

The ISE policy matrix (Work Centers > TrustSec > TrustSec Policy > Matrix**)** is a visual table showing source and destination security groups as rows and columns. Edit the policy cell to deny or restrict communication between groups, the default is to permit communication.

Figure 47 – ISE policy matrix

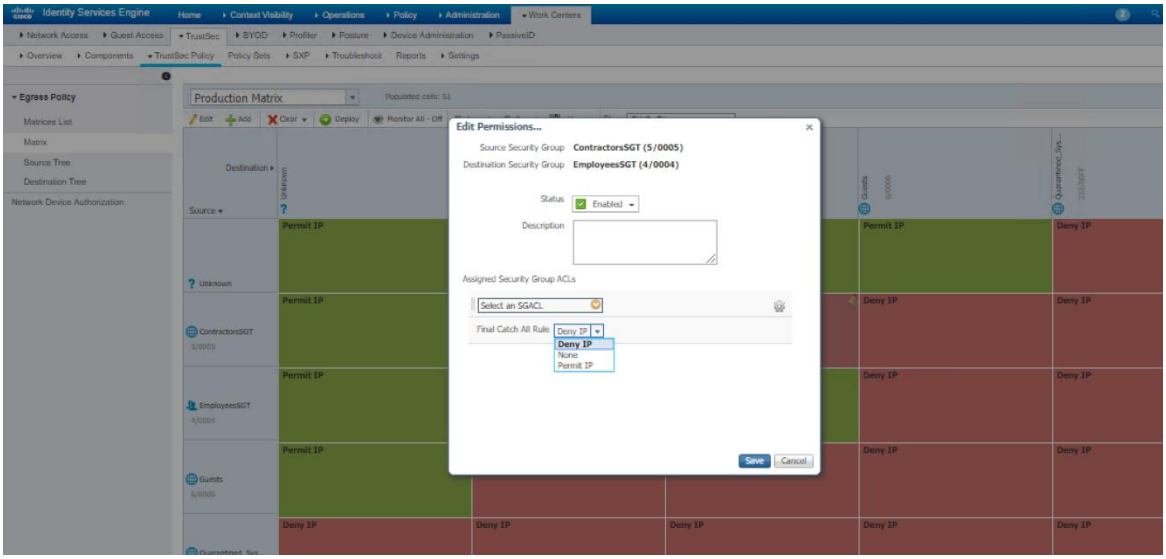


Note: I created the custom view filter to show that the SGT Unknown is considered as Internet; notice the corresponding communication flows are identical. Because TrustSec policy is not bi-directional like a firewall, you need to specifically allow or deny both directions to work.

In this example, all except quarantined devices can communicate to the Unknown, and Contractor and Employee can communicate only to Unknown and to same SGT. A Guest can communicate with only Unknown. Quarantine devices are not able to communicate with anyone. (Except we will create policy to remediate its status to Unquarantined)

Step 1 Edit the policy to permit communication between the devices. Click on the cell, click the pencil icon in the top right of the cell, select an SGACL or change the Catch All Rule. Click **Save**.

Figure 48 – Edit permissions



Step 2 After completing the policy changes, click the **Deploy** button, then the **push** button in the notification area. Click **OK** to acknowledge the CoA notifications.

EXAMPLE NOTE: If the destination device is connected to a switch without TrustSec enforcement enabled, communication is not blocked, even if a policy is configured to do so, and every other switch in the path is configured for TrustSec enforcement. Reply traffic may be blocked when returning to the source device if specified in the policy.

Security Group Tag Exchange Protocol

SXP is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically, and the SGT can be used as a classifier in network policies.

SXP uses TCP as its transport protocol to set up an SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener.

Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.

In this solution, SXP is set up in a hub-spoke fashion with all network devices peering to the ISE server for SXP. If you have firewalls between your switches and the ISE server, special configurations must be added to permit SXP through both FTD and ASA Firewalls.

Enable SXP through ASA

An SXP connection stays in the initializing state among two SXP peers interconnected by the ASA; as shown in the following example:

(SXP peer A) - - - - (ASA) - - - (SXP peer B)

Therefore, when configuring the ASA to integrate with Cisco TrustSec, you must enable the no-NAT, no-SEQ-RAND, and MD5-AUTHENTICATION TCP options on the ASA to configure SXP connections. Create a TCP state bypass policy for traffic destined to SXP port TCP 64999 among the SXP peers. Then apply the policy on the appropriate interfaces.

For example, the following set of commands shows how to configure the ASA for a TCP state bypass policy:

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options md5 allow OR tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

For more information, please visit:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/access-trustsec.html

Enable SXP through FTD

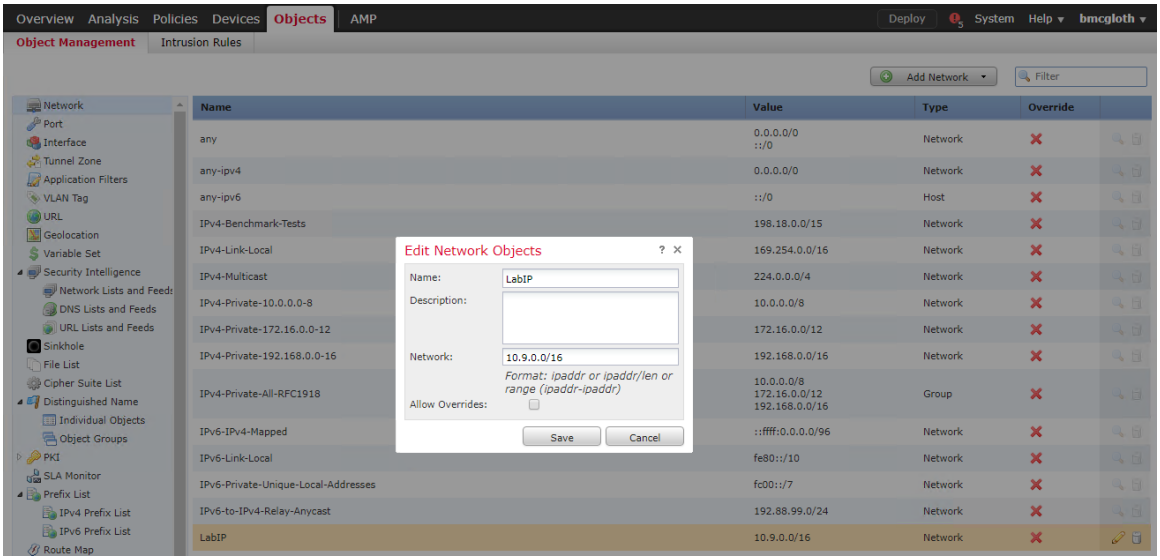
In FTD

1. Create network objects (networks and protocols)
2. Create Extended ACL
3. Create Flex-config object
4. Add Flex config object to FTD Device

Add objects for Extended Access List permitting port 64999 to all appropriate Switch IP's and ISE. In this example, we created a network object for the lab IP block.

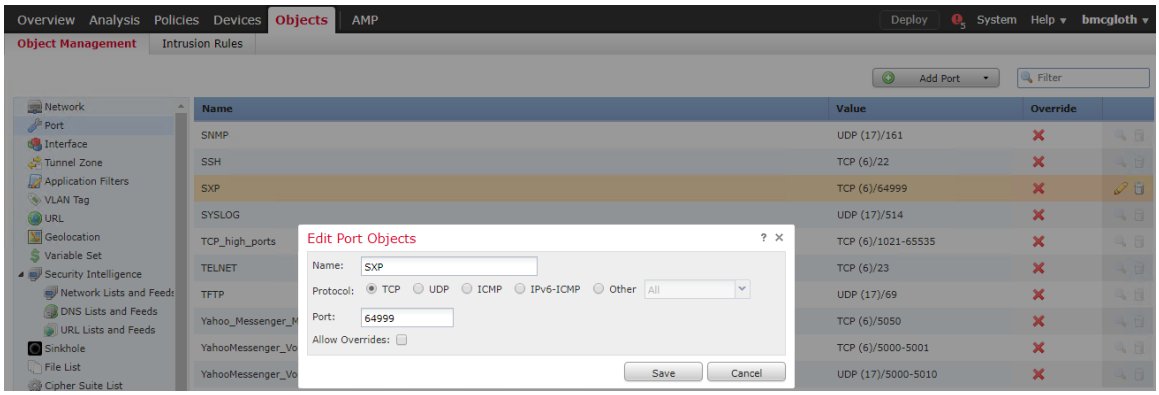
Step 1 Starting in FMC, navigate to **Objects > Object Management > Network**. Click the **Add Network** button in the upper right. Enter a Name, Description and Network. Click **Save**.

Figure 49 – Edit Network Objects



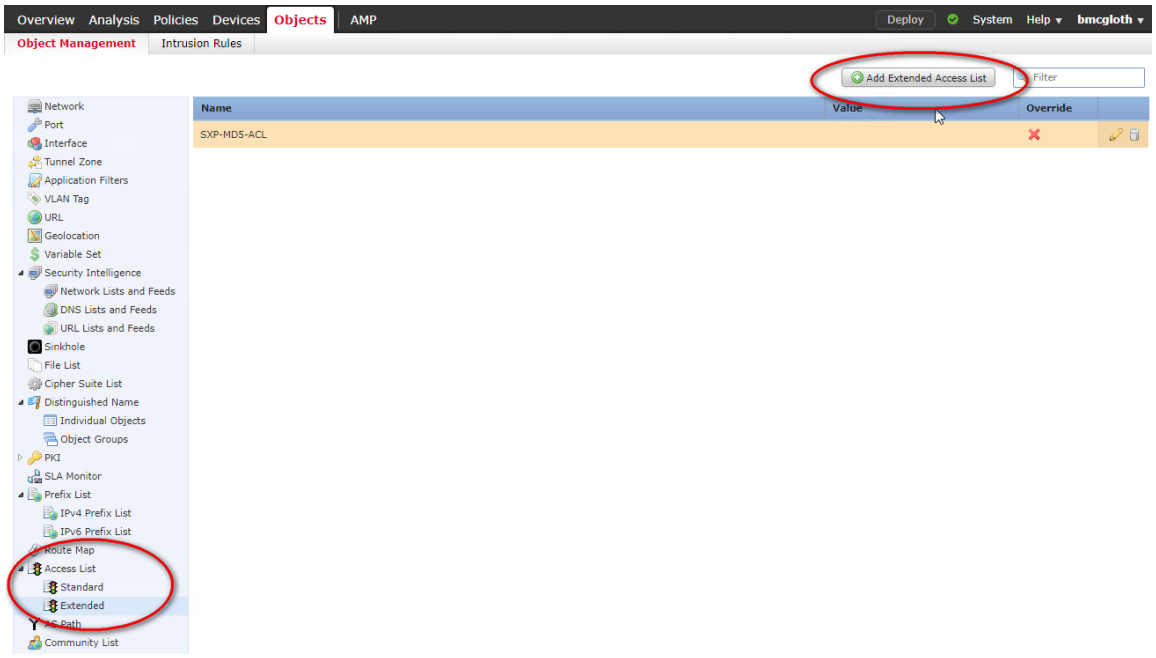
Step 2 Navigate to **Objects > Object Management > Port.** Click the **Add Port** button on the upper right. Enter the Name **SXP**, select **TCP**, Enter **64999** for the Port. Click **Save**.

Figure 50 – Edit Port Objects



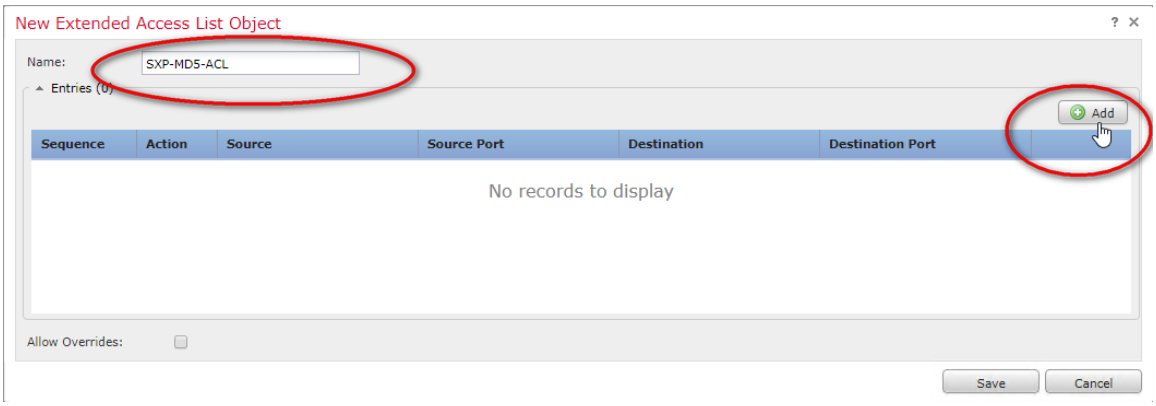
Step 3 Navigate to **Objects > Object Management > Access List > Extended.** Click the **Add Extended Access List** button in the upper right.

Figure 51 – Add Extended Access List



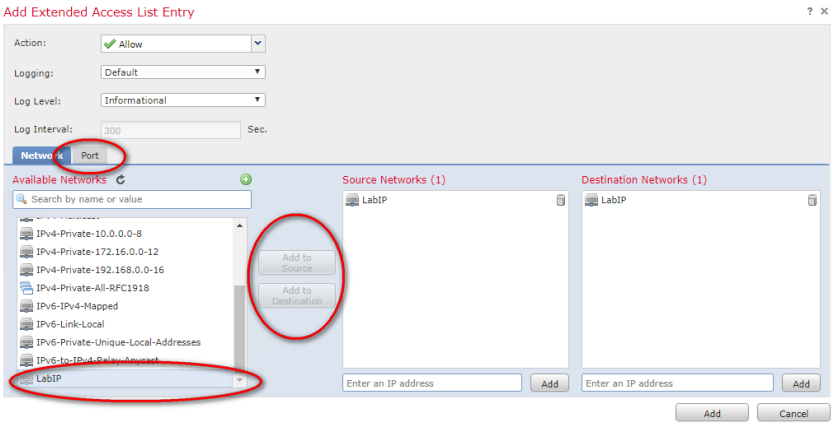
Step 4 Enter a Name. Click **Add** to start creating the access list entry.

Figure 52 – New Extended Access List Object



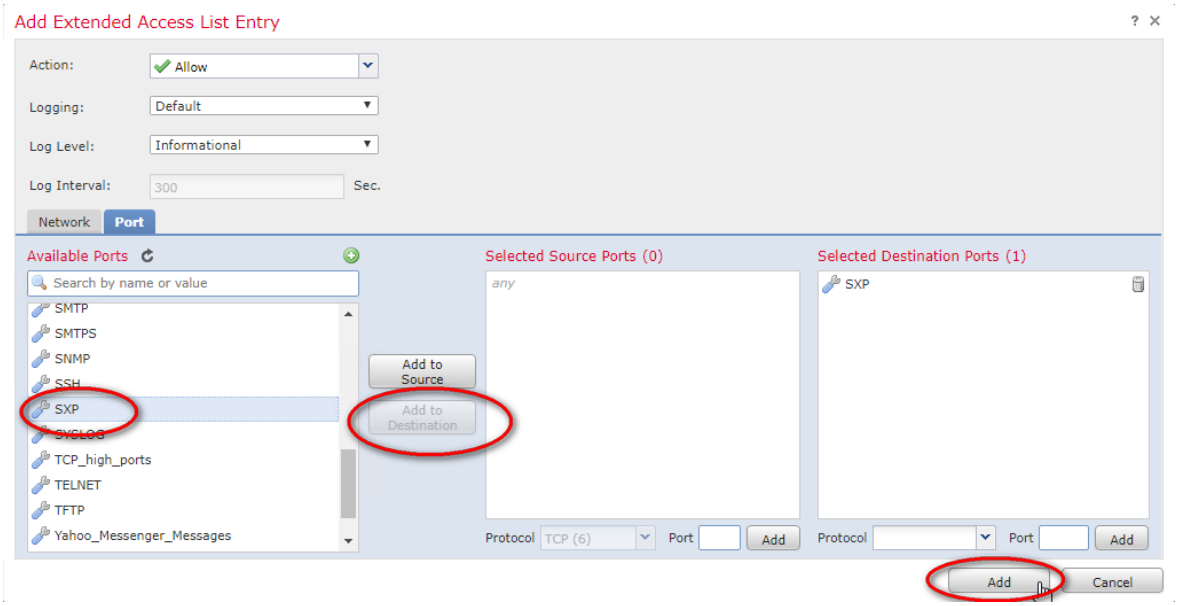
Step 5 Select the proper network object you created earlier, and add the objects to the source and destination networks as appropriate for your environment. Click the **Port** tab.

Figure 53 – Add Extended Access List Entry—Port



Step 6 Select the **SXP** port from the list of available ports, click **Add to Destination**. Click **Add** to complete the access list entry.

Figure 54 – Add Extended Access List Entry—SXP



Step 7 Navigate to **Objects > Object Management > FlexConfig > FlexConfig Object.** Click the **Add FlexConfig Object** button in the upper right. Enter a **Name**. Paste in the configs for the tcp-map and tcp-options, the class map.

```
tcp-map SXP-MD5-OPTION-ALLOW
  tcp-options md5 allow multiple

class-map SXP-MD5-CLASSMAP
  match access-list $acl
```

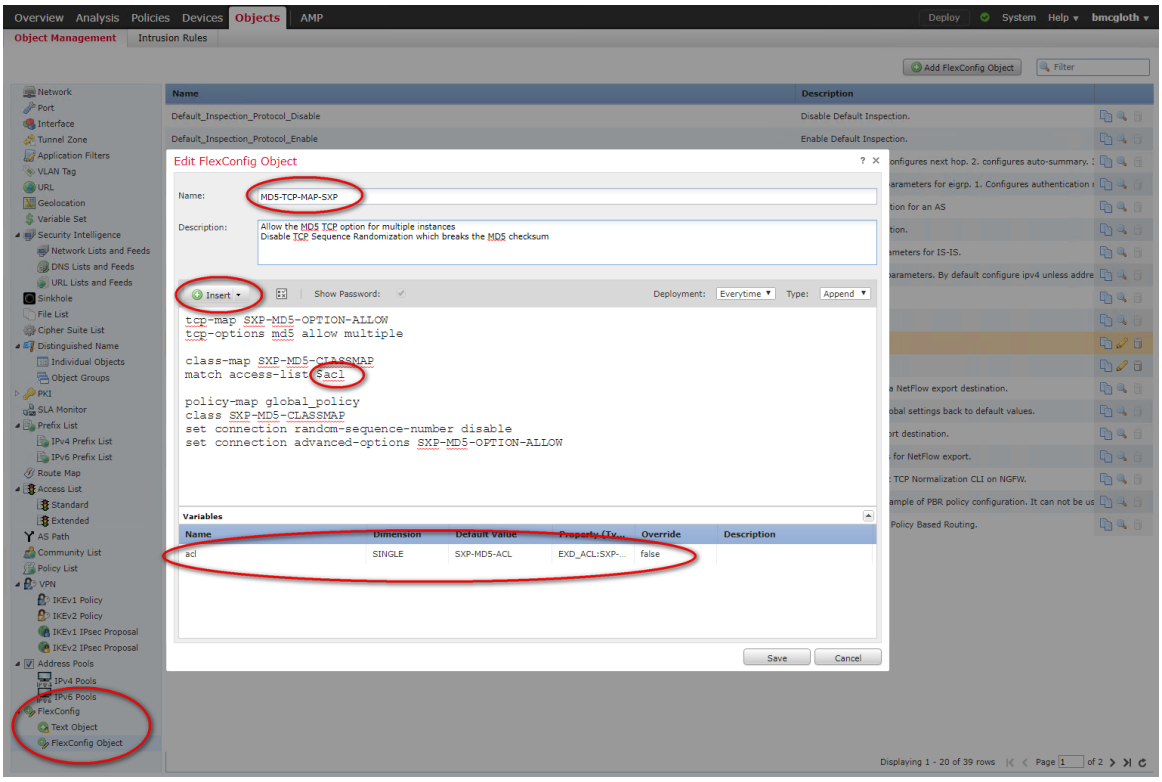
Click on **Insert** to assign the extended access list created in Step 4 as a variable: **$acl**. Paste in the global policy-map with the special connection options.

```
policy-map global_policy
 class SXP-MD5-CLASSMAP
```

```
set connection random-sequence-number disable
set connection advanced-options SXP-MD5-OPTION-ALLOW
```

Click **Save**.

Figure 55 – Edit FlexConfig Object

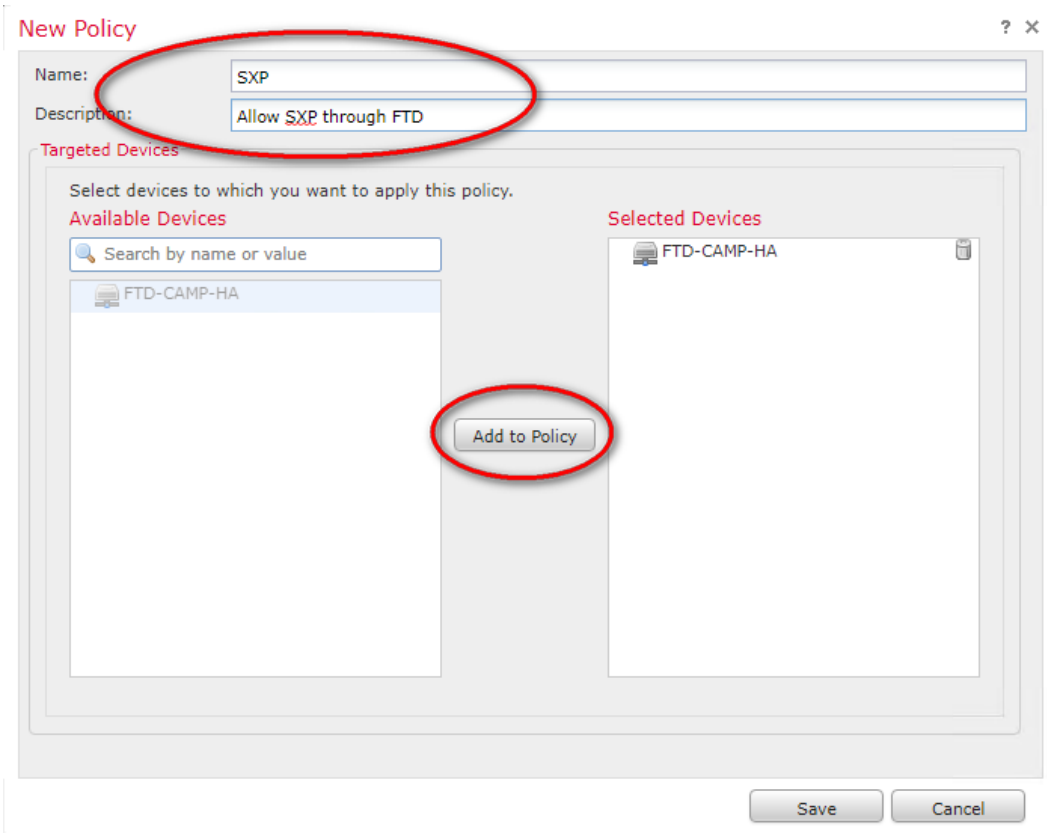


Step 8 Create a new FlexConfig policy for the devices in the network. Navigate to **Devices > FlexConfig.** Click the **New Policy** button in the upper right.

Figure 56 – Devices

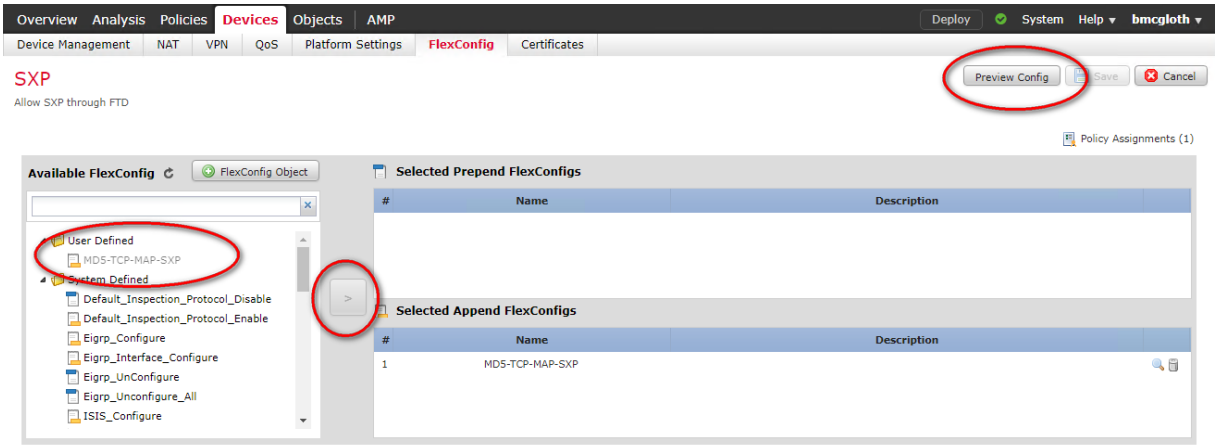
Step 8 Enter a **Name**, and optional description. Select the device from the available devices and click the **Add to Policy** button. Click **Save**.

Figure 57 – New Policy



Step 9 Select the newly defined FlexConfig from the menu on the left, click the arrow to add it to the policy. Click **Save** in the upper right, then click **Preview Config** to check the results.

Figure 58 – Add FlexConfig



Step 10 Click **Deploy** to install the new configs in the firewalls.

http://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html

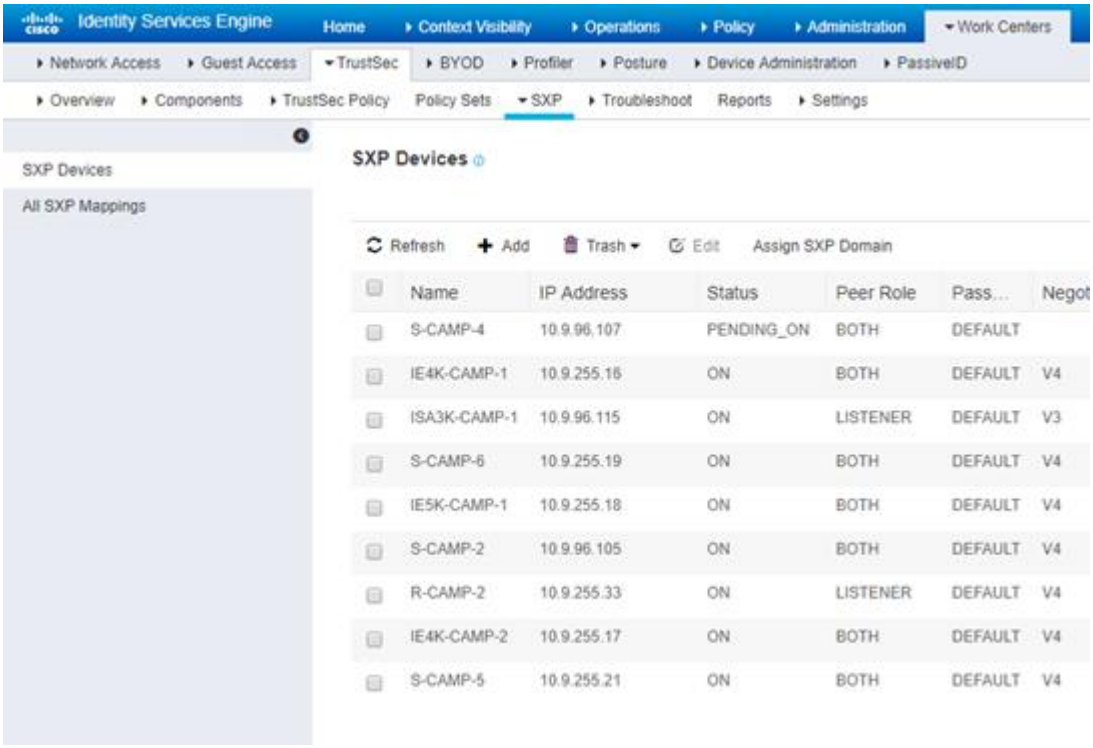
Configure SXP Device Peers in ISE

Each SXP connection has one peer designated as an SXP speaker and the other peer as an SXP listener. A best practice is to configure them in bidirectional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener. To view the SXP peer devices that are added to Cisco ISE, choose **Work centers > TrustSec > SXP > SXP Devices**.

Add network devices to ISE that will communicate with SXP.

Step 1 Starting in ISE, navigate to **Work Centers > TrustSec > SXP > SXP Devices**.

Figure 59 – SXP Devices

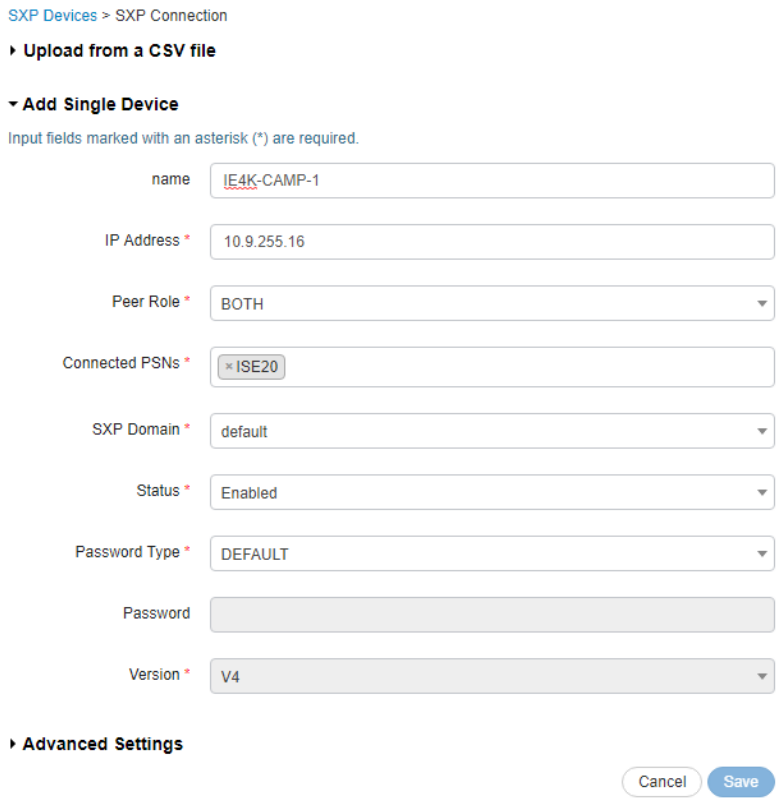


NOTE: If the corresponding network device has not been configured for SXP communication yet, the status will show as ***PENDING_ON***

Step 2 Click the **Add** button at the top of the list.

Step 3 Enter the Name, IP address, Peer Role, PSN and Password for each switch or firewall that will connect to ISE using SXP.

Figure 60 – SXP Devices



NOTE: The SXP global default password can be specified instead of different device specific passwords. To set the Global Password navigate to **Work Centers > TrustSec > Settings > SXP Settings.**

Step 4 Click **Save**.

Configure SXP on network devices

The following example shows how to enable SXP and configure an SXP peer connection between the ISE PSN, the speaker, and a Switch or ASA, the listener:

Step 1 Specify the Cisco TrustSec device ID and password for this switch to use when authenticating with ISE and establishing the PAC file. This password and ID must match the ISE Network Devices configuration specified earlier. At the device command line enter:

```
cts credentials id {switch ID} password Cisco123
```

Step 2 You first enable Cisco TrustSec SXP before you can configure peer connections.

```
cts sxp enable
```

Step 3 As a best practice, specify the source IP address and configure a default password.

```
cts sxp default source-ip {loopback or interface IP}
     cts sxp default password Cisco123
```

NOTE: If a default SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco TrustSec software derives the SXP source IP address from existing local IP addresses. The SXP source address might be different for each TCP connection initiated from the switch.

Step 4 Configure the SXP peer connection to the ISE PSN. If the device does not support peer mode **BOTH**, configure peer as **SPEAKER**. Make sure to use the same password on both ends.

```
cts sxp connection peer ISEPSN password default mode peer both
```
or
```
cts sxp connection peer ISEPSN password default mode peer speaker
```

Step 5 Verify the SXP connection is established

```
 show cts sxp connections
```

Displays detailed information about the SXP status and connections.

```
IE4K-CAMP-2#sh cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: 10.9.255.17
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 10.9.10.51
Source IP        : 10.9.255.17
Conn status      : On (Speaker) :: On (Listener)
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Speaker Conn hold time   : 120 seconds
Listener Conn hold time   : 120 seconds
Local mode       : Both
Connection inst# : 1
TCP conn fd      : 1(Speaker) 2(Listener)
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 19:03:19:52 (dd:hr:mm:sec) :: 19:03:19:28
(dd:hr:mm:sec)

Total num of SXP Connections = 1
```

Enable TrustSec enforcement

The following configurations add enforcement capabilities to the switches.

Step 1 Configure the switch to use RADIUS authorization for all network-related service requests.

```
aaa authorization network cts-list group ISE
```

Step 2 Specify the TrustSec AAA server group for cts authorizations.

```
cts authorization list cts-list
```

Step 3 Specify the SGT for the switch to use for its own traffic.

```
cts sgt 2
```

Step 4 Enable role-based enforcement globally and per VLAN.

```
cts role-based enforcement
cts role-based enforcement vlan-list 115-117
```

Step 5 Enable routing globally on the switch:

```
ip routing
```

Step 6 Before enabling inline tagging on switch interfaces, the SDM mode must also be changed to routing. Check the current mode using the **`show sdm prefer`** command.

```
IE4K-CAMP-2#sh sdm prefer
 The current template is "default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

       number of unicast mac addresses:                  16K
       number of IPv4 IGMP groups + multicast routes:    1K
       number of IPv4 unicast routes:                    18K
         number of directly-connected IPv4 hosts:        16K
         number of indirect IPv4 routes:                 2K
       number of IPv6 multicast groups:                  0
       number of IPv6 unicast routes:                    0
         number of directly-connected IPv6 addresses:    0
         number of indirect IPv6 unicast routes:         0
       number of IPv4 policy based routing aces:         0.125k
       number of IPv4/MAC qos aces:                      1.875k
       number of IPv4/MAC security aces:                 1.875k
       number of IPv6 policy based routing aces:         0
       number of IPv6 qos aces:                          0
       number of IPv6 security aces:                     0
```

Step 7 If the SDM mode is not set to “routing”, enter configuration mode and enter the following global command:

```
sdm prefer routing
```

After entering the command, you will receive the following notification:

```
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

Step 8 Save the switch configuration and reload the switch.

```
Copy running-config startup-config
reload
```

Step 9 After the switch has reloaded, enable manual TrustSec tagging for uplinks. Enable propagation of leaned SGT’s (default) and manually tag unknown traffic with a defined SGT, and trust tagged packets received.

```
interface GigabitEthernet1/16
 cts manual
  propagate sgt
  policy static sgt 37 trusted
```

“trusted” indicates that ingress traffic on the interface should not have its tag overwritten.

NOTE: In ISE, an SGT should be created to identify untagged traffic that may transit between systems. Create SGT for OTHER_UNTAGGED traffic when doing inline tagging, in our example tag 37 was dynamically assigned from the ISE pool. Add new Security Groups by navigating in ISE to **Work Centers > TrustSec > Components > Security Groups**

Step 10 TrustSec enforcement happens on the egress port of the switch with attached device, so enforcement should be disabled on Switch to Switch and uplink Trunk port interfaces. The following example disables role-based enforcement:

```
interface GigabitEthernet1/16
 switchport trunk allowed vlan 115-117
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 cts manual
  propagate sgt
  policy static sgt 37 trusted
 no cts role-based enforcement
```

TrustSec Troubleshooting commands are as follows:

- show cts interface brief
- sh cts sxp sgt-map brief
- sh cts role-based counters
- sh cts role-based permissions
- show cts role-based sgt-map all
- cts refresh policy
- cts refresh environment-data

show authentication interface gigabitEthernet 2/1
show mab interface gigabitEthernet 2/1 details

TrustSec Troubleshooting Guide
https://communities.cisco.com/docs/DOC-69479

pxGrid configuration

Best practices for configuring and deploying pxGrid can be found here:

- The Cisco Platform Exchange Grid (pxGrid) provides a highly secure system for other technologies to exchange intelligence.
- Firepower—Rapid Threat Containment

Firepower Threat Defense (FTD) Policy

In the previous Quick Prevention Ransomware Defense Solution, we introduced the use of Cisco Umbrella and AMP for Endpoint for both DNS and web security. In addition to these endpoint protections, the Advanced Ransomware Defense solution provides network web security using categorized URL filtering and security intelligence features that work with Talos.

What is the difference between a URL Filtering block/interactive block and a Security Intelligence block?

Security Intelligence decisions are one of the first things the NGFW does. Whether it is an IP address, a domain, or a URL, if a packet is seen with a simple match on any of these three items, the connection is blocked. URL filtering decisions are made in access control policies, which is both a later function in the detection process and can be widely varied based on how the AC policy is made. URL filtering data and security intelligence data are two different data sets. URL filtering data is based on categorization and potential risk (e.g., Gambling, Adult, Hacking, and News; as well as the level of risk associated with any listing). Security intelligence data is published by Talos based on observed and known threats.

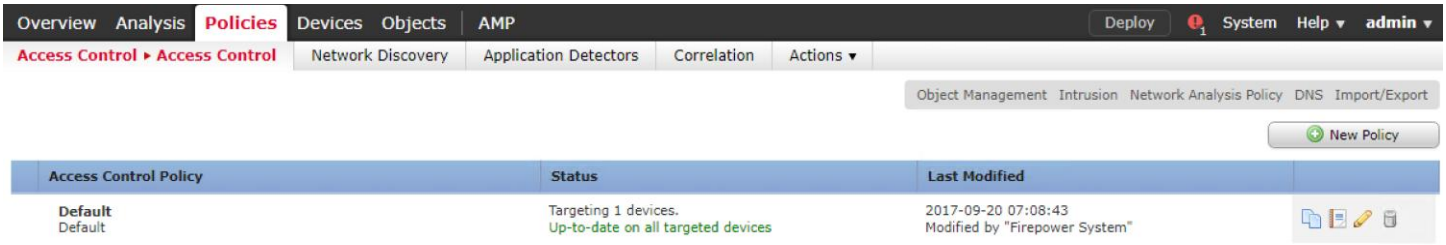
In this sample policy, Employees are able to connect to any internet URLs with the exception of categories blocked by corporate policy (Gambling, Peer to Peer, Malware and Hacking). If a system is placed in Quarantine, all outbound web connectivity is blocked except that destined for the corporate support site “cleanme.cisco-x.com”. pxGrid enables the use of SGTs as the traffic source, providing a greatly simplified policy without the need to specify networks and device IP addresses.

Now we'll add a rule to allow the devices to send telemetry to the corporate data lake in the cloud over HTTP and HTTPS.

In Firepower Management Center, policies for next-generation firewalls and next-generation IPS systems are configured under the **Policies > Access Control > Access Control Policy > Default**.

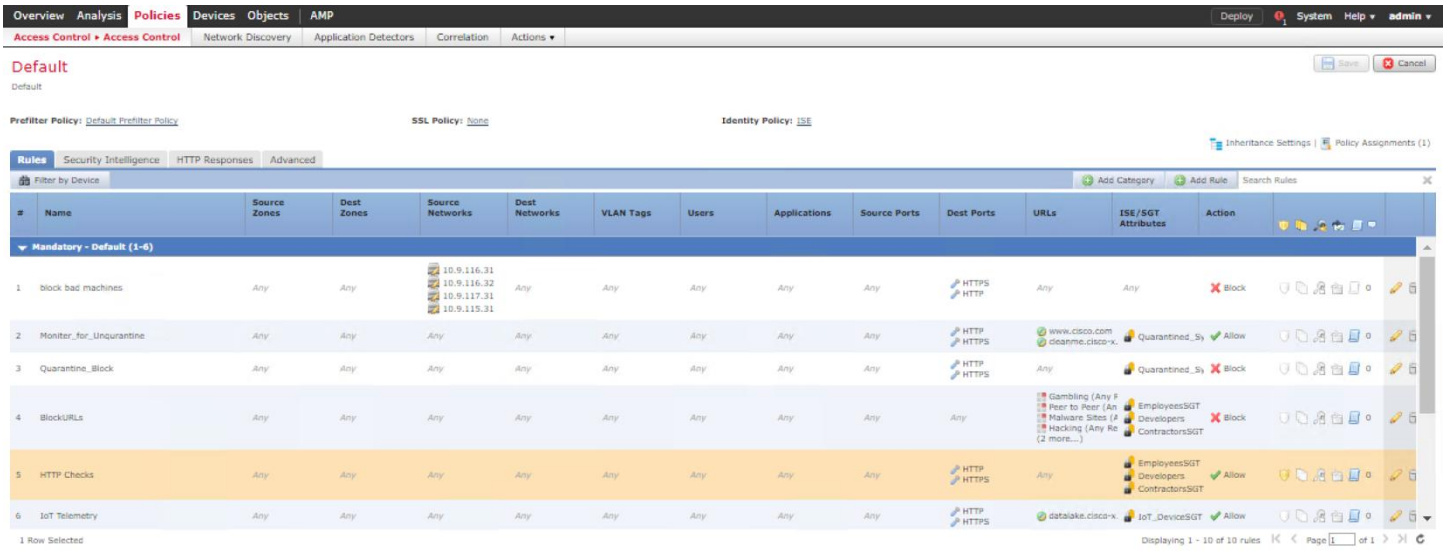
Step 1 Edit the existing policy by clicking on the pencil on the right, or create a new policy.

Figure 61 – Policies



Step 2 Click the **Add Rule** button at the top of the policy rules.

Figure 62 – Policies—Add Rule



Step 3 Create policy as follows in the Default Policy:

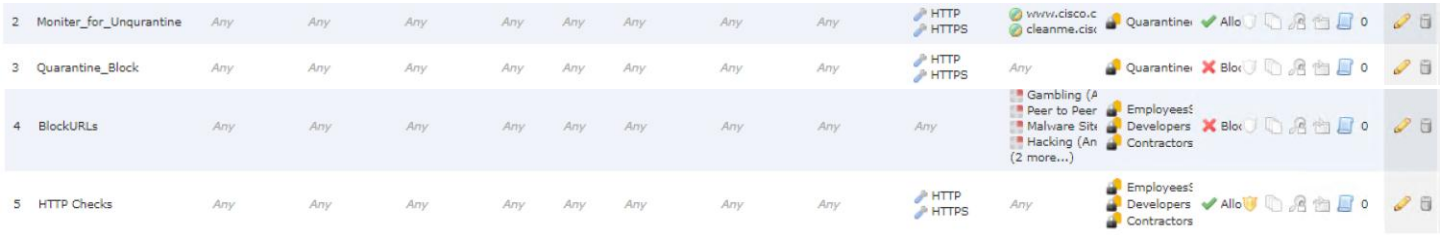
Name	Action	Source	Destination	Protocols
Allow Internal	Allow	Inside and Outside ZONE	Inside and Outside ZONE	Any

Figure 63 – Default Policy—Policies

In the Mandatory Policy top to bottom:
(In order to select SGT as a criterion, you need to configure pxGrid to retrieve SGT data from ISE)

Name	Action	Destination Ports	URLs	ISE/SGT Attribute	Note:
Monitor_for_ Unquarantine	Allow	HTTP/HTTPS	www.cisco.com/ cleanme.cisco-x.com	Quarantined.System	To allow the quarantined.system to be unquarantined by accessing to the specific URLs
Quarantine_Block	Block	HTTP/HTTPS	Any	Quarantined.System	Deny everything else for the quarantined.system
Block URLs	Block	Any	Categories: Gambling/Peer to Peer/Malware/ Hacking	EmployeeSGT DevelopersSGT ContractorSGT	Block categorized URL groups for Employee/ Developer and Contractor SGT
HTTP Checks	Allow	Any	Any	EmployeeSGT DevelopersSGT ContractorSGT	Allowing everything else on HTTP/HTTPS

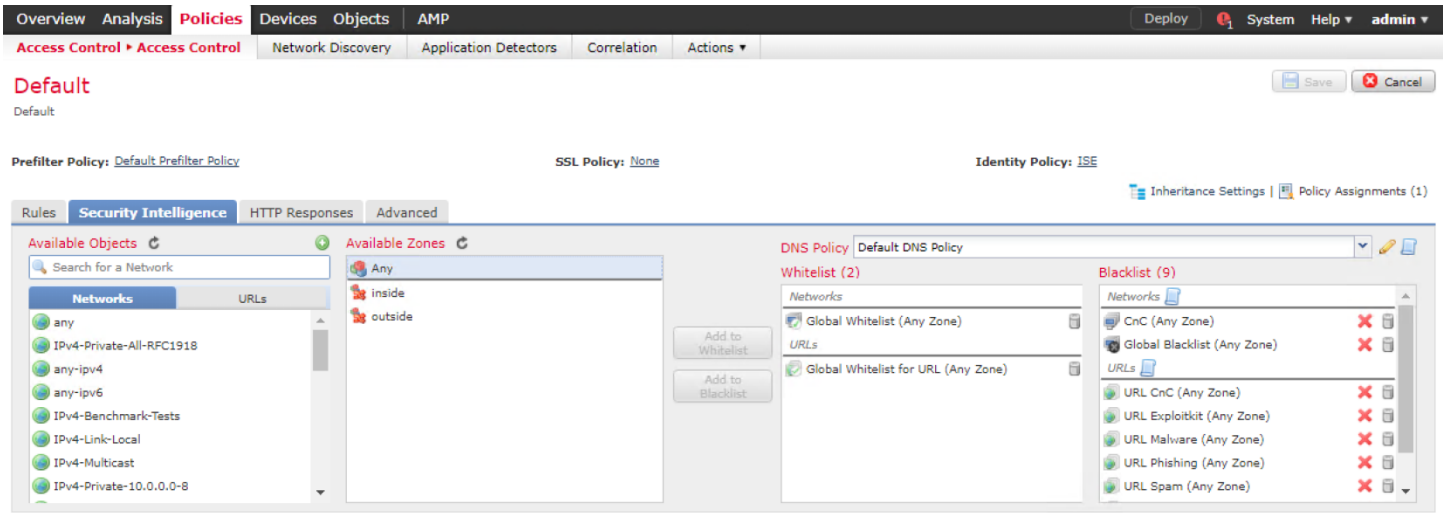
Figure 64 – Policies



Step 4 Next to the Rule tab, select the **Security Intelligence** tab to create the Threat Intelligence policy under the **Policies > Access Control > Access Control Policy > Default**.

In the Available Object search box, Search for CnC and Global Blacklist for Networks. And add them to blacklist. Search URL for URLs. Add them to the blacklist. (URL CnC, Exploitkit, Malware, Phishing, Spam, Suspicious and Global Blacklist for URL. Applied to all zones)

Figure 65 – Security Intelligence



Stealthwatch

Cisco Stealthwatch uses NetFlow to provide visibility across the network, data center, branch offices, and cloud. Its advanced security analytics uncover stealthy attacks on the extended network. Stealthwatch helps you use your existing network as a security sensor and enforcer to dramatically improve your threat defense.

Cisco Stealthwatch with Threat Intelligence

Cisco Stealthwatch uses NetFlow data as input to help organizations detect behaviors linked to a wide range of attacks, including advanced persistent threats (APT), distributed denial-of-service (DDoS), and insider threats.

Better Visibility and Contextual Threat Intelligence

Cisco ISE delivers enhanced visibility and contextual information on network activities. It helps accelerate threat identification by sharing NetFlow and ISE contextual data with Cisco Stealthwatch. You can go from mapping IP addresses to understanding threat vectors based on who, what, where, when, and how users and devices are connected, and how they access network resources.
Using the Cisco network infrastructure as a security sensor gives you a powerful and scalable solution to gain deep visibility, control, and analytics.

The deployment described is based on several design and deployment guides that comprise the reference network architecture:

- Cisco Cyber Threat Defense v2.0 Design Guide
- Configuring pxGrid in an ISE Distributed Environment Guide
- Deploying Cisco Stealthwatch 6.7.1 with Cisco pxGrid Guide
- User-to-Data-Center Access Control Using TrustSec Deployment Guide
- Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide

Following is the example configuration of a NetFlow Record in a Cisco Catalyst 3850 switch.
For other device configuration, please refer to the NetFlow configuration page.

To define the NetFlow Record, use the following commands:

```
flow record StealthWatch_Record
    description NetFlow record format to send to StealthWatch
    match datalink mac source address input
    match datalink mac destination address input
    match datalink vlan input
    match ipv4 ttl
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
```

To define the NetFlow Exporter, use the following commands:

```
flow exporter StealthWatch_Exporter
    description StealthWatch Flow Exporter
    destination <FlowCollector_Address>
    source <Loopback_Interface>
    transport udp 2055
```

To define the NetFlow Monitor, use the following commands:

```
flow monitor StealthWatch_Monitor
    description StealthWatch Flow Monitor
    record StealthWatch_Record
    exporter StealthWatch_Exporter
    cache timeout active 60
```

Finally, assign the Flow Monitor to every interface where you're interested in monitoring traffic:

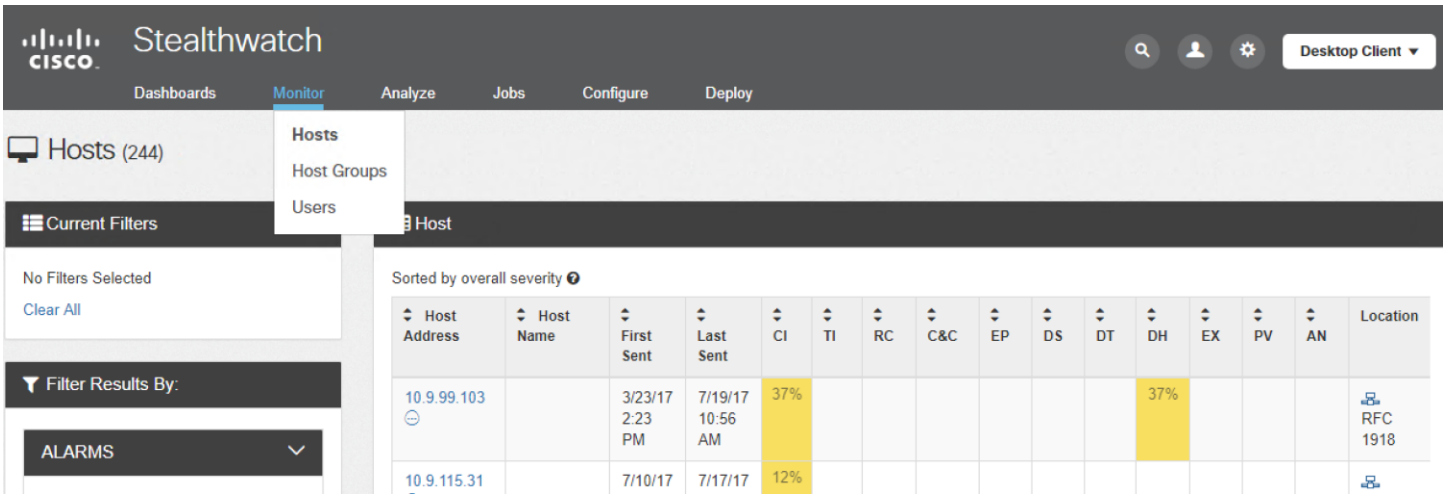
```
interface <Interface_or_VLAN>
    ip flow monitor StealthWatch_Monitor input
```

Stealthwatch and ISE integration

With pxGrid between ISE and Stealthwatch, a network administrator can monitor and analyze host-based activities with information provided by ISE such as specific username and SGT names. Upon analysis, suspicious host activities can be identified and the administrator can easily quarantine the subject to prevent further threats within the network.

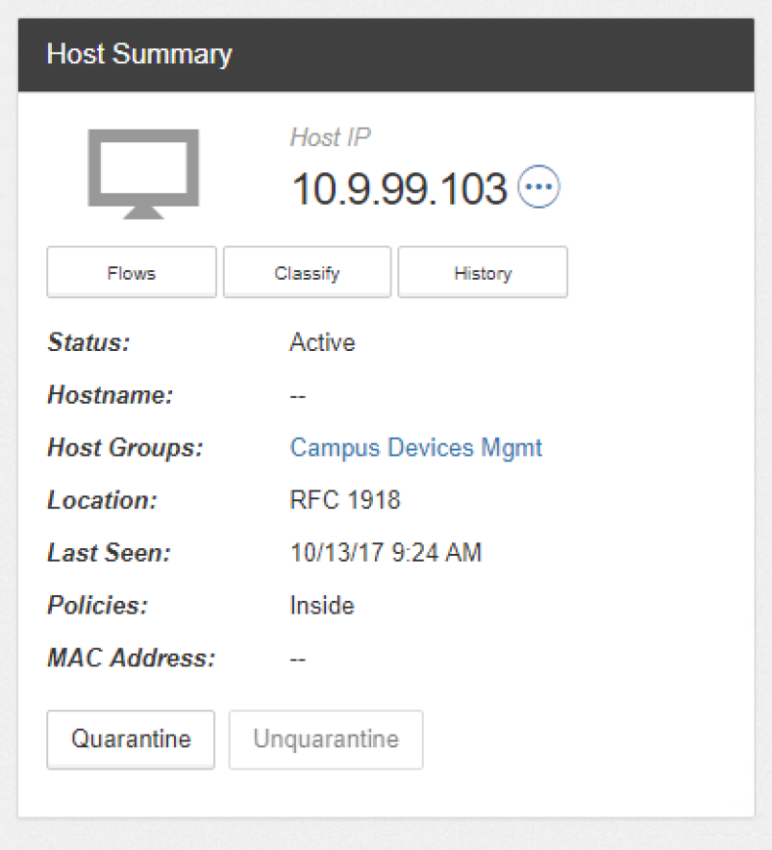
Go to the the SMC Dashboard under **Monitor > Hosts**.

Figure 66 – Monitor > Hosts



Select one of the IP address links to access a host summary where you will find the quarantine button. Select this button to initiate a request to change the STG towards ISE.

Figure 67 – Host Summary



Validation Testing

Solution validation testing for the first phase of the design was accomplished by creating a representative enterprise network of Windows servers and Client workstations with full internet connectivity.

Testing implemented Cisco's Cloud Email Security, DNS Security with Umbrella, and AMP for endpoints products.

Before testing the samples of ransomware, servers and workstations were deployed and joined to an Active Directory domain. File shares were configured from the workstations to file servers, and mapped to a drive letter. Microsoft Exchange was deployed for the email server, and email accounts were created for users unique to each workstation deployed. Various software packages were installed on the systems to best represent several typical generations of infrastructure deployments and upkeep as specified in Table 5.

Table 5 - Test system software installations

Test system software installations versions:							
	XPsp3x86	Win7sp1x64 Enterprise	Win10x64 Enterprise	2008R2 LOW-FS	2012R2 HIGH-FS	2012R2 AD	2012R2 Exchange
Java	Jre-6u45	Jre-7u80	Jre-8u91				
MS Office	2007	2013	2016				
Firefox	5	20	47				
MS IE	8	10	11	8	11	11	11
Acrobat Reader	10	11	DC				
Adobe Flash	12	18	21				
MS .net	2	3.5	4.5	3.5	3.5+4.5		3.5+4.5
MS Silverlight	3	4	5.1				
C++	9.0.3	9.0.3	9.0.3				
Host FW	Off	Off	Off	Off	Off	Off	Off
DNS to AD	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Join AD	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Static IP and GW	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Twenty-one families of ransomware samples were run on these systems to establish a baseline of what ransomware would infect each system build, whether administrative user rights were needed, and how quickly the encryption completed for local and network shares.

None of the working ransomware samples needed to perform a DNS lookup before encrypting the system. It is believed that this is because the known samples used have had their C2 domains already shut down or moved, so those samples did not function on the baseline systems, and were removed from further testing.

As all test samples were obtained from the Threat Grid File analysis repository, they were immediately recognized by AMP when the files were SHA-256 hashed by the connector and checked. To create unique versions of the ransomware for testing, a re-hashing utility was used which modified the executable files and inserted innocuous spaces or annotations, changing the resulting file hash without affecting the operation ability of the ransomware samples. This allowed testing of automatic file analysis features for low prevalence files in all products.

Advanced Ransomware Solution Validation Testing

In addition to our Quick Prevention Ransomware Defense solution, which includes Cisco Cloud Email Security, Cisco Umbrella, and Cisco AMP for Endpoint, the advanced Ransomware Solution includes mostly appliance-based Cisco security products lines, as shown in Table 6.

Table 6 – Advanced Ransomware Solution validation testing

Product	Description	Platform
Stealthwatch	Collect and analyze NetFlow	Virtual or Appliance
ISE	Authenticate and Profile devices connecting to network	Virtual or Appliance
Cognitive Threat Analytics	Analysis of Flows from SW	Cloud
Firepower Management Center	Manage Firepower Threat Defense systems	Virtual or Appliance
Firepower Threat Defense	Security platforms running Firepower Threat Defense software image	Virtual and 2100, 4100, 9300
ASA	Firewall	ASA5500-X
ASA-ASDM	Local FW Mgmt	ASA5500-X
NGIPS on ASA	Protection and Control	ASA5500-X
AnyConnect	Secure Mobility Client	All
Catalyst Switches	Aggregation	6880 6807-XL
	Access	3650, 3850

Solution component implementation

In this advanced phase, we set up following components and features:

1. Firepower Threat Defense with Threat Intelligence features
2. Cisco Identity Service Engine (ISE)
3. Cisco TrustSec
4. Cisco Stealthwatch

For the Advance Ransomware testing, we built a group of Windows-based clients and a few servers including mail, file, and Active Directory servers. These Windows-based clients are Windows XP, Windows 7, and Windows 10. Windows 2008 server and Windows 2012 Servers are also built to deliver the ransomware through email and file sharing.

Testing objective

This Advanced Ransomware solution testing is created to validate the effective identification of the malicious communication between the corporate clients/servers and outside internet servers that may host malware and ransomware, or other components such as exploit kits to infect the device/network.

Furthermore, setting multiple layers of segmentation points will prevent worm-based ransomware from infecting the various segments of the network.

Testing setup and each component role

FTD and ISE

Both FTD and ISE will be the security policy enforcement points. FTD will have a multiple access policy that includes base inbound and outbound access control that can be set by the specific customer requirements. FTD access policies also include those managed with the ISE security tagging as source and destination. The policy based on the Security Tagging will be used to enforce when the specific host becomes subject to the “Change of Authorization” by ISE (Quarantined).

In addition, FTD has a policy for the Talos Threat Intelligence functions. This feature will allow FTD to monitor any outbound traffic (mainly HTTP and HTTPS) that may be malicious.

To provide rapid threat containment functions, there is a pxGrid relationship between FTD and ISE.

ISE and TrustSec

Security tag policy set in the ISE will be downloaded towards supported Cisco switches to provide base security group tagging segmentation. These SGACLs are carefully configured at different layers of switches. These SGACL also include source tags as “Quarantined”. The SGACL will be in effect only when the applied tagged packets were transmitted.

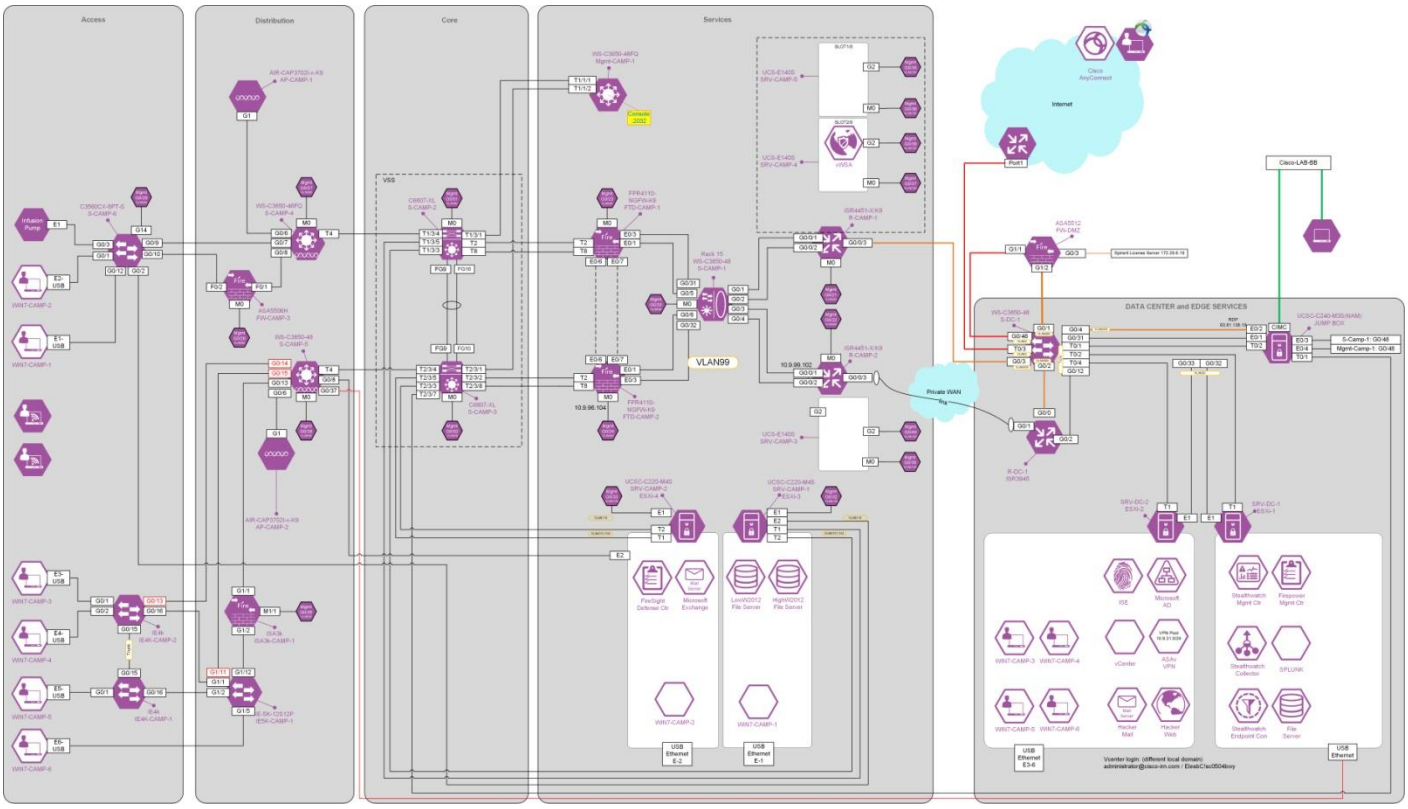
ISE and Stealthwatch

Similar to the relationship between FTD and ISE, we have setup PXGrid between ISE and Stealthwatch. With this setup, under the Stealthwatch traffic analysis report, the administrator can identified the source object with actual client authenticated user name which information was pushed from ISE database. Furthermore, from the StealthWatch’s host detail report, administrator can initiate the change of authorization to ISE. ISE will then change the host tag to be “Quarantined”.

Network Topology

Network topology includes all the components explained above.

Figure 68 – Network topology



Validation Testing

Summary of Tests Performed

These tests are designed to validate the integration of and general functionality of various Cisco Security products against ransomware. Our methods of the validation process are based on the layers of service applied over the network.

The following table outlines the tests conducted to validate the deployment.

Table 2 Test Scenarios

Test	Methodology
Deploy and enforce Security Group Tag ACL into the Switch using ISE	Policies are created in the ISE to propagate SGACL into the supported Cisco Switch. SXP was used to dynamically allocated.
Tag internal host using ISE local authentication	ISE has authenticated user by active directory then assigned “Employee” tag to be enforced. All the users whom access the network through VPN client will be tagged as “VPN User”
Validate COA by ISE upon user access C2 malicious web site	FTD to monitor internal device access to Command and Control malicious web site. Once FTD flags the action, it will request COA to ISE which it will change the tagging of the particular host from “Employee” to “Quarantine”
Validate method to be Unquarantined	Set a policy in FTD that Quarantine device will have limited access. In addition, set a policy in the ISE quarantine device to unquarantined by accessing certain web site as a proof.
Manual quarantine/unquarantine using host device reporting page of Stealthwatch Management Console	Identify tagged host/s and execute quarantine/unquarantine action from SMC.
VPN Tagging	Apply Security Group Tagging towards users onboarding by remote access VPN connections.
Cisco Identity Services Engine (ISE) Integration	Confirm integration of the ISE with the components listed below with PXGrid. • ISE authentication and authorization services across the infrastructure – Nexus switching – UCS Domain – FTD Platforms – Stealthwatch

Summary of results

The following table lists a summary of the results of testing.

Table 3 Summary of Results

Test Description	Components	Result
Internal host tagging	ISE, RADIUS, Active Directory	User was successfully tagged upon authentication
VPN user tagging	ISE, RADIUS, Active Directory	User was successfully tagged upon authentication
TrustSec setup (SGACL Download)	ISE, Supported Switch	SGACL set in the ISE were successfully uploaded into supported cisco switches
SXP and policy enforcement at the switch setup	ISE, Supported Switch	Was able to allow or deny traffic based on the TrustSec policy set in the ISE servers
COA with FTD and ISE	FTD, ISE	Through FTD threat intelligence feature, successfully client device accessed to the C2 malicious site were identified by FTD and ISE to COA the device to be quarantined. Quarantined devices access managed by SGACL at the switch level as well as in FTD.
Automatic Unquarantine device	ISE, FTD, Quarantined device, Unquarantine website	Successfully unquarantine the device by visiting website which included in the ISE policy for the unquarantine method.
Manual Quarantine/Unquarantine with StealthWatch Management Console	Stealthwatch Management Console, ISE	Successfully quarantine/unquarantine device from StealthWatch Management Console manually

Summary

Ransomware is a problem that will continue to grow and impact more organizations. If attacks are successful, they create a significantly negative business impact on an organization.

This solution accomplishes the goal of keeping your organization up and running, with the peace of mind that there is only a small chance of losing control of your critical systems and being held hostage.

The period of time from a new malicious campaign starting to Threat intelligence-based protection is 30 min-4hr with the Cisco Ransomware Defense Solution, significantly better than the industry average of 100 days[4]. Cisco Ransomware Defense focuses on prevention where possible, quick detection, and rapid containment to reduce the impact of a ransomware attack if one gets through your defenses.

[4] http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html?KeyCode=001031927

References

Cisco SAFE Simplifies Security:
www.cisco.com/go/safe

Cisco Cloud Email Security:
http://www.cisco.com/web/products/security/cloud_email/index.html
Cisco Email Security:
http://www.cisco.com/c/en/us/products/security/email-security/index.html
Cisco Email URL content filtering best practices:
http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html

Cisco DNS Security:
https://www.opendns.com/enterprise-security/threat-enforcement/
Cisco Umbrella Roaming Client Installation:
http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf
DNS Best Practices:
http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html
Setting up DNS Forwarding for Windows Server 2012 and 2012 R2:
https://support.opendns.com/entries/47071344-Windows-Server-2012-and-2012-R2

Cisco Advanced Malware Protection for Endpoints:
http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html
Cisco Advanced Malware Protection:
http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Cisco Talos - Comprehensive Threat Intelligence:
http://www.cisco.com/c/en/us/products/security/talos.html
Cisco ThreatGrid:
http://www.cisco.com/c/en/us/solutions/enterprise-networks/amp-threat-grid/index.html

Cisco Web Security:
http://www.cisco.com/c/en/us/products/security/web-security/index.html

Network as a Sensor:
http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-sensor.html
Cisco Stealthwatch:
http://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
Cisco Identity Services Engine with TrustSec (Network as an Enforcer):
http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-enforcer.html
Cisco Rapid Threat Containment Solution:
http://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

Cisco Firepower Management Center:
http://www.cisco.com/c/en/us/products/security/firesight-management-center/index.html