EASY NAC

FEATURE BRIEF - AUTOMATED THREAT RESPONSE

With Malware Lateral Spread Protection – Zero Day

www.easynac.com

V3.1 211231

Automated Threat Response

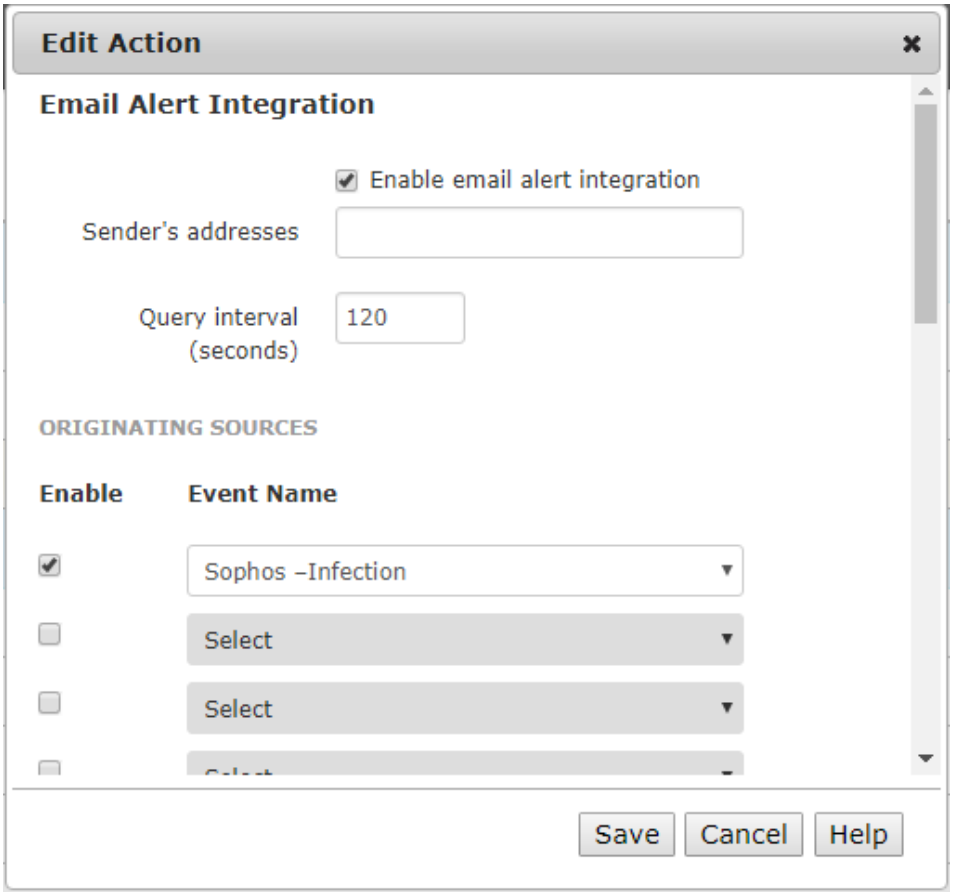
Firewalls, IPS, APT, SIEM and many other security solutions are designed to monitor devices and network traffic and send event-based alerts for administrative action. Firewalls and APT solutions can often block the malicious traffic at the gateway level, but this can still leave the internal network vulnerable to the threat.

Easy NAC can protect the internal network from threats by immediately restricting the offending device so it would be unable to send traffic to other devices on or off the local subnet. CGX Access will receive e-mail alerts or event-based syslog messages from all types for security devices and take immediate action to quarantine the device.

A key benefit of the CGX Access design, is its ability to work with any security solution that can send e-mail or syslog messages. No special versions or APIs required, just an e-mail will do.

Orchestration with Email Alerts

E-mail alerts are a standard mechanism that most security solutions use to notify administrators of critical events or threats. CGX Access can use these same e-mails to enable Automated Threat Response. CGX Access can receive e-mail messages from all types for security devices and take immediate action when necessary. Any solution that can send email messages can be configured to work with CGX Access.

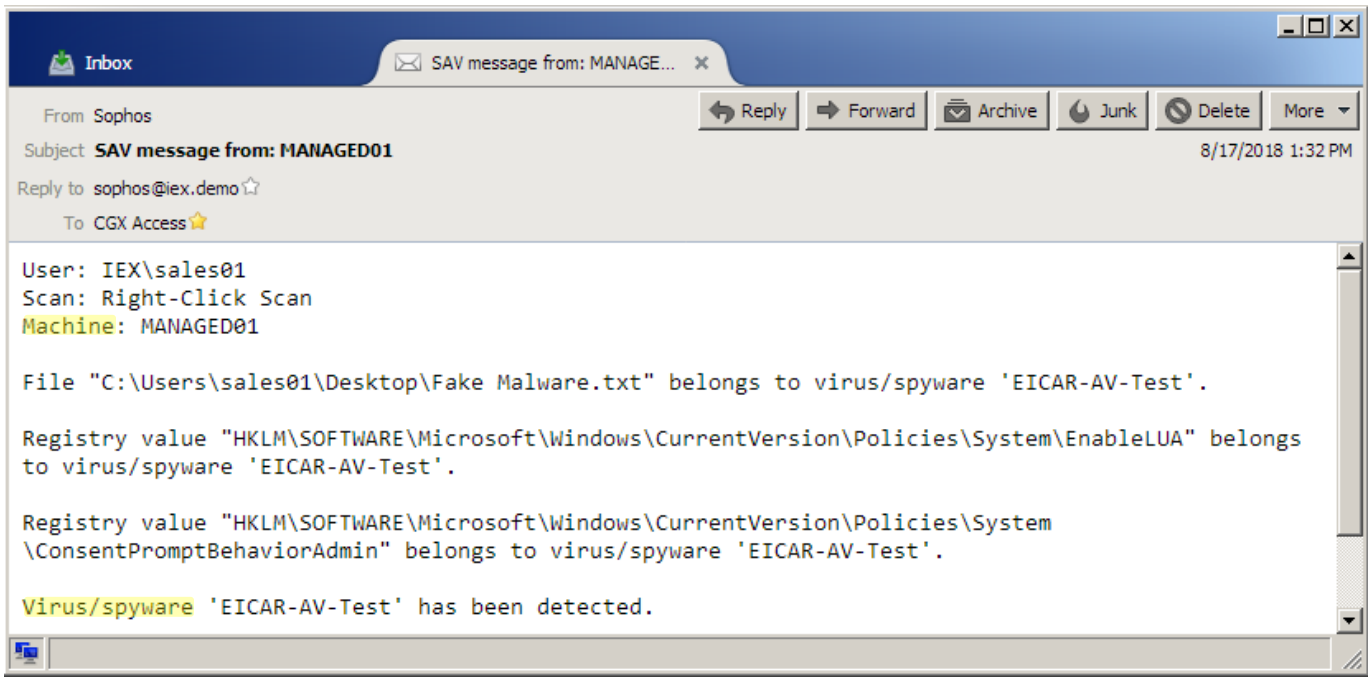


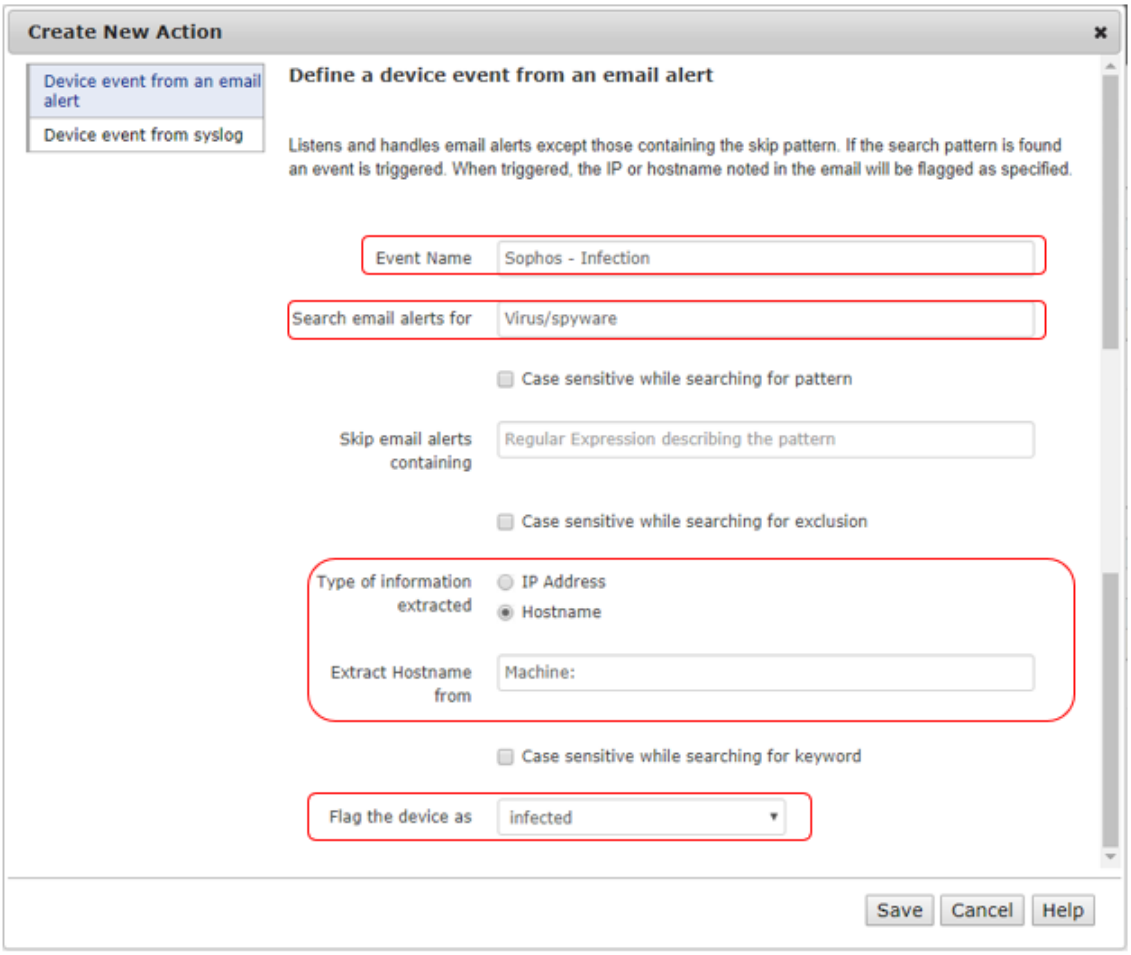
From the E-mail integration screen shown above, numerous events can be enabled for the CGX Access appliance to monitor. These events are easy to create and customized, so CGX Access knows exactly what e-mails to take action on.

Event Creation – E-mail

CGX Access can work with any solution (Firewall, APT, IPS, SIEM, AV, etc.) that can send e-mail alerts. To setup an event, administrator can specify what are the keywords or phase that CGX should detect when reading an e-mail. Configuring E-mail events are simple, as you only need a sample e-mail to create the event.

Below is a sample e-mail of an alert sent by an AV server. We can simply review this email to identify the keywords, and then use them to create an event.





The example above defined a device event to read e-mail messages for the key phrase “Virus/Spyware”. If this phase is seen, an Infected flag will be assigned to the Hostname of the malware-infected device.

Policy-Based Response

Continuing with the above example, CGX Access will take real-time quarantine actions based the flag that has been assigned. Using policy defaults, a device flagged with an Infected flag will be assigned Restricted access.

Automated Device Classification Policy

Activate | Cancel Changes

Classify devices based on their characteristics

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set device role to full-access	
Device is on whitelist	Set device role to full-access	
Device is on blacklist	Set device role to restricted	
Has any of these flags: APT-Event, FP-mismatched, FW-Event, infected, IPS-Event, SIEM-Event	Set device role to restricted because Malware or Suspicious Behavior has been detected	
Zero-Day Threat	Set device role to High-Risk-Event because Suspicious network activity detected	
Passed Agent Audit	Set device role to full-access	
Failed Agent Audit	Set device role to failed-agent-audit	
Has any of these flags: AV-off, AV-out-of-date	Set device role to non-compliant because Device is NOT compliant with the corporate Anti-Virus policy.	
Has any of these flags: patch-failed, patch-pending	Set device role to non-compliant because Device is NOT compliant with the corporate Patch Management policy.	
Has any of these flags: VoIP, AD-managed, AV-managed, full-access, managed-device, network-infrastructure, printer, router, switch	Set device role to full-access	
Completed Guest or Device Registration Has any of these flags: byod	Set device role to BYOD	
Completed Guest or Device Registration Has any of these flags: consultant	Set device role to consultant	
Completed Guest or Device Registration	Set device role to guest	

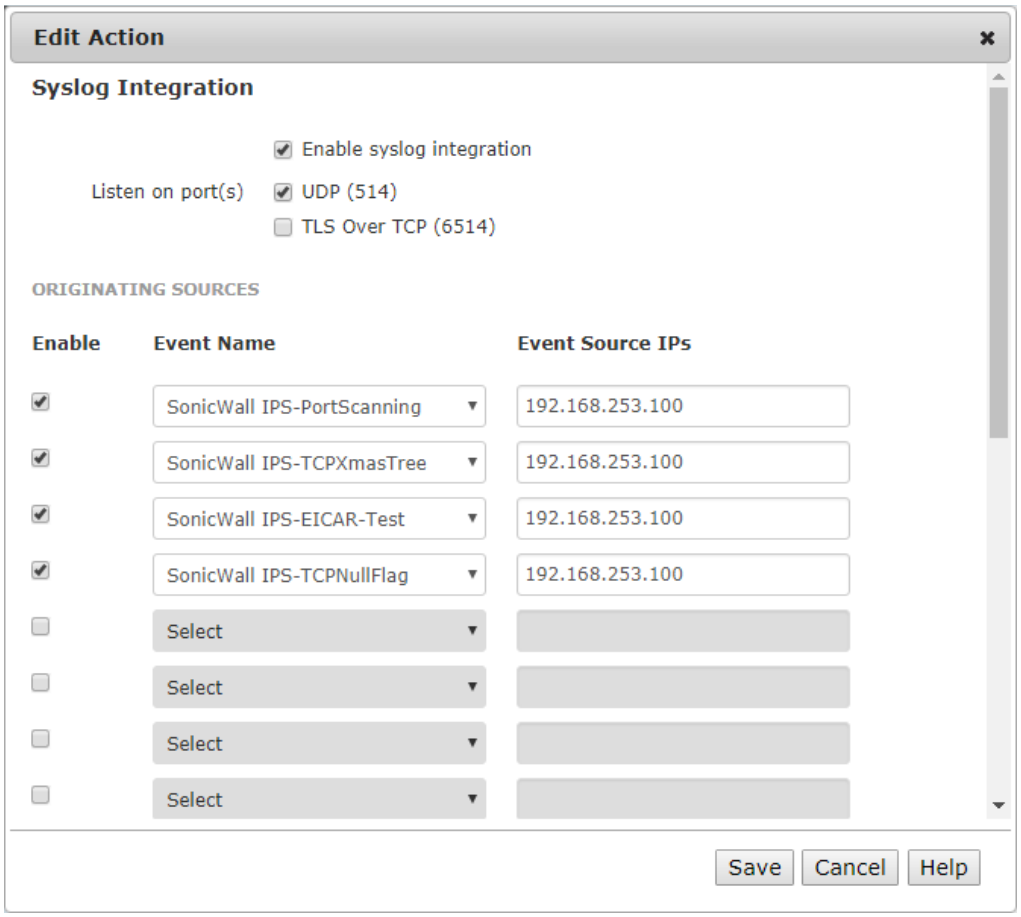
Below is the automated response, where MANAGED01 was flagged as being infected and immediately assigned restricted access.

MAC	Hostname	Events	Access Group	Roles	Location	IP Address	OS	Flags / Lists	Last Seen	Access Status	Grant Access
00:0C:29:4B:70:2E	MANAGED01	2018-08-18 18:49:25 Sophos – Infection (infected)	restricted	restricted	Demo	192.168.253.54	Windows 7 Professional	virtual AD-managed infected	2018-08-18 20:13:57		ON OFF Auto

Conditions	Actions taken when conditions are met
Device is on whitelist	Set device role to full-access
Device is on blacklist	Set device role to restricted
Has any of these flags: APT-Event, FW-Event, **infected**, IPS-Event, SIEM-Event	Set device role to restricted

Orchestration with Syslog

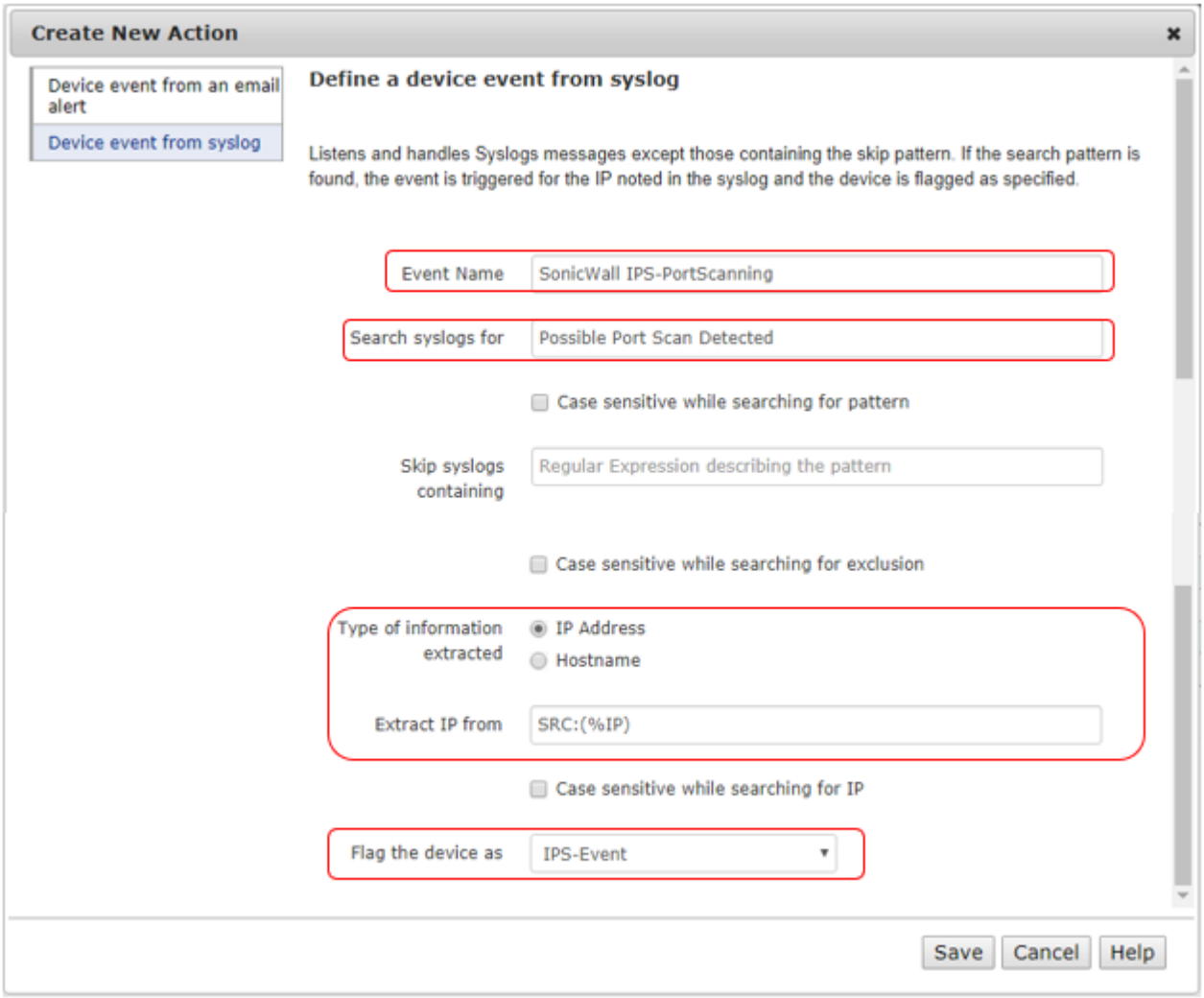
Any solution that can send event-based syslog messages can be configured to work with Easy NAC. CGX Access can be configured to listen to syslog messages from approved IP address(es)



From this Syslog Integration screen, numerous events can be enabled for the CGX Access appliance to monitor. These events are easy to create and customized, so CGX Access knows exactly what it should listen for.

Event Creation - Syslog

To setup an event, the administrator can specify what are the keywords or phase that CGX should search for inside the syslog message.



The example above defines a device event to search syslog messages for the key phrase “Possible Port Scan Detected”. If this phase is seen, an IPS-Event flag will be assigned to the IP address of the mis-behaving device. In this event, the IP address follows the keyword SRC:

Policy-Based Response

Continuing with the above example, CGX Access will then take real-time quarantine actions based the flag that has been assigned. Using policy defaults, a device flagged with an "IPS-Event" will be assigned Restricted access.

Automated Device Classification Policy

Activate | Cancel Changes

Classify devices based on their characteristics

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set device role to full-access	
Device is on whitelist	Set device role to full-access	
Device is on blacklist	Set device role to restricted	
Has any of these flags: APT-Event, FP-mismatched, FW-Event, infected, IPS-Event, SIEM-Event	Set device role to restricted because Malware or Suspicious Behavior has been detected	
Zero-Day Threat	Set device role to High-Risk-Event because Suspicious network activity detected	
Passed Agent Audit	Set device role to full-access	
Failed Agent Audit	Set device role to failed-agent-audit	
Has any of these flags: AV-off, AV-out-of-date	Set device role to non-compliant because Device is NOT compliant with the corporate Anti-Virus policy.	
Has any of these flags: patch-failed, patch-pending	Set device role to non-compliant because Device is NOT compliant with the corporate Patch Management policy.	
Has any of these flags: VoIP, AD-managed, AV-managed, full-access, managed-device, network-infrastructure, printer, router, switch	Set device role to full-access	
Completed Guest or Device Registration Has any of these flags: byod	Set device role to BYOD	
Completed Guest or Device Registration Has any of these flags: consultant	Set device role to consultant	
Completed Guest or Device Registration	Set device role to guest	

Below is the automated response, where 192.168.253.54 was flagged as having an IPS-event and immediately assigned restricted access.

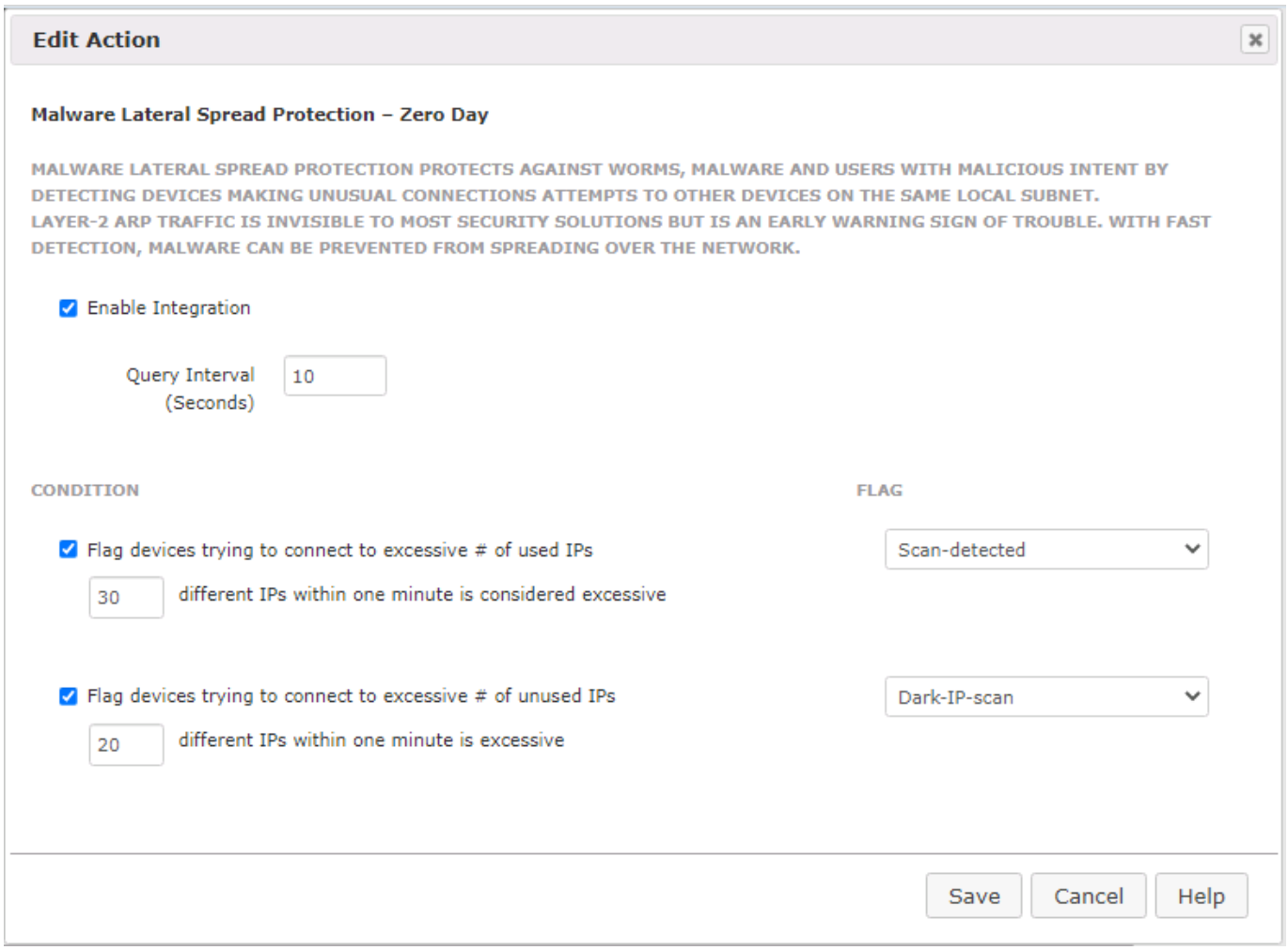
MAC	Hostname	Events	Access Group	Roles	Location	IP Address	OS	Flags / Lists	Last Seen	Access Status	Grant Access
00:0C:29:4B:70:2E	MANAGED01	2018-08-18 16:42:49 SonicWall IPS-PortScanning (IPS-Event)	restricted	restricted	Demo	192.168.253.54	Windows 7 Professional	virtual AD-managed IPS-Event	2018-08-18 16:57:34		ON OFF Auto

Conditions	Actions taken when conditions are met
Device is on whitelist	Set device role to full-access
Device is on blacklist	Set device role to restricted
Has any of these flags: APT-Event, FW-Event, infected, **IPS-Event**, SIEM-Event	Set device role to restricted

Malware Lateral Spread Protection - Zero-day

During its normal operation, the CGX Access appliances are listening to broadcast traffic on the end-user segments. With this layer-2 visibility, CGX Access is in a unique position to detect devices making unusual connection attempts to other devices within the same segment. If an end-user device suddenly attempts to connect to an excessive number of devices on the same subnet, or trying to connect to Dark IPs that at not active on the network, this is very suspicious behavior. This behavior is indicative of a network scan being performed or malware trying to probe the network in an attempt to spread. Easy NAC can detect this behavior and immediately quarantine this device so it can't spread malware laterally on the network.

With no integration or special requirements, this detection is easy to enable. Devices attempting connection attempts to an excessive number of hosts will be flagged as "Scan-detected". While devices attempting connection attempts to unused IP addresses will be flagged as "Dark-IP-Scan"



Policy-Based Response

When the "Scan-detected" flag and "Dark-IP-Scan" flag is assigned to a device, the CGX Access can then take real-time quarantine actions based on Device Classification policies. In the Policy shown below, any device that has been flagged as a zero-day threat will immediately be assigned the High-Risk role and restricted.

Automated Device Classification Policy

Activate | Cancel Changes

Classify devices based on their characteristics

Add Rule

Conditions	Actions taken when conditions are met
Device is on routerlist	Set device role to full-access
Device is on whitelist	Set device role to full-access
Device is on blacklist	Set device role to restricted
Has any of these flags: APT-Event, FP-mismatched, FW-Event, infected, IPS-Event, SIEM-Event	Set device role to High-Risk-Event because Malware or Suspicious Behavior has been detected
Zero-Day Threat	Set device role to High-Risk-Event because Suspicious network activity detected
Passed Agent Audit	Set device role to full-access
Failed Agent Audit	Set device role to failed-agent-audit
Has any of these flags: AV-off, AV-out-of-date	Set device role to non-compliant because Device is NOT compliant with the corporate Anti-Virus policy.
Has any of these flags: patch-failed, patch-pending	Set device role to non-compliant because Device is NOT compliant with the corporate Patch Management policy.
Has any of these flags: VoIP, AD-managed, AV-managed, full-access, managed-device, network-infrastructure, printer, router, switch	Set device role to full-access
Completed Guest or Device Registration Has any of these flags: byod	Set device role to BYOD
Completed Guest or Device Registration Has any of these flags: consultant	Set device role to consultant
Completed Guest or Device Registration	Set device role to guest

Below is the automated response, where 10.160.0.22 was flagged as having both a Scan-detected and Dark-IP-Scan. It was immediately assigned and High-Risk role with restricted access.

MAC	Hostname	Comment	Events	Access Group	Roles	IP Address	OS	Flags / Lists	Last Seen	Access Status	Grant Access
00:50:56:AF:A3:D8	desktop-6fjp5su	AD Client	2022-01-16 20:46:13 arpscan (Scan-detected) 2022-01-16 20:46:13 darkip (Dark-IP-scan)	High-Risk	High-Risk-Event	10.160.0.222	WinX64 10 Enterprise 6.3 Build 19043 Service Pack None	AD-managed virtual Scan-detected Dark-IP-scan	2022-01-16 20:46:24		ON OFF Auto

Conditions	Actions taken when conditions are met
Device is on excludelist	Set device role to excluded
Device is on routerlist	Set device role to full-access
Device is on whitelist	Set device role to full-access
Device is on blacklist	Set device role to restricted
Has any of these flags: APT-Event, FP-mismatched, FW-Event, infected, IPS-Event, SIEM-Event	Set device role to High-Risk-Event because Malware or Suspicious Behavior has been detected
Has all of these flags: **Dark-IP-scan**, **Scan-detected**	Set device role to High-Risk-Event because Suspicious network activity detected

Summary

Automated Threat Response is a powerful feature to help stop malicious malware from spreading. If a device is detected to have ransomware, it is not enough to restrict the device at the gateway level, it's critical to isolate that machine from the rest of the network as quickly as possible to prevent the lateral spread of the malware. Easy NAC provides this level of protection, so a device can be isolated immediately from all other devices on the network.

Easy NAC's Automated Threat Response features are more flexible and responsive than other NAC orchestration features for three key reasons:

1) CGX Access can integrate with **any** 3rd-party security appliance that can send e-mail alerts. No special APIs, modules or licensing is required.

2) CGX Access unique layer-2 visibility of the network allows for the immediate detection of suspicious behavior and immediate protection from zero-day malware propagating on the network.

3) ATR features are only effective if you have a strong quarantine mechanism that can be implemented. Easy NAC's plug and protect design provides protection at the edge of the network with no network changes or network configurations required.

Easy NAC's ARP enforcement mechanism is easy to implement, while providing immediate detection and strong enforcement at the edge of the network. It's this real-time enforcement mechanism that provides the foundation for its strong Automated Threat Response features.