ISE en FirePower-integratie - voorbeeld van servicesherstel

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren Netwerkdiagram **FirePOWER** FireSIGHT Management Center (Defense Center) Toegangsbeheerbeleid ISE-servicemodule voor vernieuwing Correlatiebeleid **ASA** ISE Netwerktoegangsapparaat (NAD) configureren Adaptieve netwerkcontrole inschakelen **Quarantine DACL** Licentieprofiel voor Quarantine machtigingsregels Verifiëren AnyConnect start ASA VPN-sessie Toegang tot gebruikerspogingen FireSight Correlatie Policy Sit ISE voert guarantaine uit en zendt CoA toe VPN-sessie is losgekoppeld VPN-sessie met beperkte toegang (guarantaine) Problemen oplossen FireSight (defensiecentrum) ISE Bugs Gerelateerde informatie Gerelateerde Cisco Support Community-discussies

Inleiding

Dit document beschrijft hoe u de servicemodule op een Cisco FireSight-apparaat kunt gebruiken om aanvallen te detecteren en de aanvallen automatisch te herstellen met het gebruik van de Cisco Identity Services Engine (ISE) als beleidsserver. Het voorbeeld dat in dit document wordt gegeven, beschrijft de methode die wordt gebruikt voor het herstel van een externe VPN-gebruiker die via ISE authentiek verklaart, maar het kan ook worden gebruikt voor een bekabelde of draadloze gebruiker 802.1x/MAB/Webex.

Opmerking: De aanpassingsmodule waarnaar in dit document wordt verwezen wordt niet officieel ondersteund door Cisco. Het wordt gedeeld op een communautair portaal en kan door iedereen gebruikt worden. In versies 5.4 en hoger is er ook een nieuwere herstelmodule beschikbaar die is gebaseerd op het *pxGrid*-protocol. Deze module wordt niet ondersteund in versie 6.0, maar zal naar verwachting in toekomstige versies worden ondersteund.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco adaptieve security applicatie (ASA) VPN-configuratie
- Cisco AnyConnect Secure Mobility Client-configuratie
- Cisco FireSight-basisconfiguratie
- Cisco FirePower-basisconfiguratie
- Cisco ISE-configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco ASA versie 9.3 of hoger
- Cisco ISE-softwareversies 1.3 en hoger
- Cisco AnyConnect Secure Mobility Client versies 3.0 en hoger
- Cisco FireSIGHT Management Center versie 5.4
- Cisco FirePOWER versie 5.4 (virtuele machine)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Gebruik de informatie in dit gedeelte om het systeem te configureren.

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het in dit document beschreven voorbeeld gebruikt deze netwerkinstellingen:



172.16.31.206

Dit is de stroom voor deze netwerkinstellingen:

- 1. De gebruiker start een externe VPN-sessie met de ASA (via Cisco AnyConnect Secure Mobility versie 4.0).
- 2. De gebruiker probeert toegang te krijgen tot *http://172.16.32.1*. (Het verkeer verloopt via FirePower, dat op de VM is geïnstalleerd en wordt beheerd door FireSight.)
- 3. FirePower is zo geconfigureerd dat het dat specifieke verkeer blokkeert (inline)

(toegangsbeleid), maar heeft ook een correlatiebeleid dat wordt geactiveerd. Als resultaat hiervan start het ISE-herstel via REST Application Programming Interface (API) (de *QuarantineByIP*-methode).

- 4. Zodra ISE de REST API-oproep ontvangt, zoekt zij naar de sessie en stuurt zij een RADIUSwijziging van autorisatie (CoA) naar de ASA, die die sessie beëindigt.
- 5. De ASA ontkoppelt de VPN-gebruiker. Aangezien AnyConnect is ingesteld met een altijd-on VPN-toegang, wordt een nieuwe sessie ingesteld; deze keer wordt echter een andere ISE Authorization-regel (voor in quarantaine gehouden hosts) aangepast en wordt de beperkte toegang tot het netwerk geboden. In dit stadium is het niet van belang hoe de gebruiker zich aansluit op en authentiek verklaart op het netwerk; zolang de ISE wordt gebruikt voor verificatie en autorisatie, heeft de gebruiker beperkte toegang tot het netwerk als gevolg van quarantaine.

Zoals eerder vermeld, werkt dit scenario voor elk type geauthentiseerde sessie (VPN, bekabeld 802.1x/MAB/Webauth, draadloos 802.1x/MAB/Webauth) zolang ISE voor authenticatie wordt gebruikt en het apparaat voor netwerktoegang de RADIUS CoA (alle moderne Cisco-apparaten) ondersteunt.

Tip: U kunt de gebruiker uit quarantaine plaatsen door de ISE GUI te gebruiken. Toekomstige versies van de saneringsmodule zouden dit ook kunnen ondersteunen.

FirePOWER

Opmerking: Een VM-apparaat wordt gebruikt voor het voorbeeld dat in dit document wordt beschreven. Alleen de eerste configuratie wordt via de CLI uitgevoerd. Alle beleid wordt geconfigureerd vanuit Cisco Defense Center. Raadpleeg het gedeelte <u>Verwante informatie</u> van dit document voor meer informatie.

De VM heeft drie interfaces, één voor beheer en twee voor inline inspectie (intern/extern).

Al het verkeer van de VPN-gebruikers beweegt via FirePower.

FireSIGHT Management Center (Defense Center)

Toegangsbeheerbeleid

Nadat u de juiste licenties hebt geïnstalleerd en het FirePower-apparaat hebt toegevoegd, navigeer dan naar **Beleid > Toegangsbeheer** en maakte u het toegangsbeleid dat wordt gebruikt om het HTTP-verkeer naar 172.16.32.1 te laten vallen:

| Overview Analysis Polic | Devices Ob | ects AMP | | | | | | | | | 😔 Heath – Sy | stem Help | v ad | nin v |
|---|-----------------|-----------------|--------------------|------------------|----------------|----------|--------------|-----------|------------|----------------------------|----------------|---------------------------------|----------|-------|
| Access Control Intrusion | Files Network | k Discovery SSL | Application Deb | ectors Users | Correlation Ac | ttipes = | | | | | | | | |
| AccessPolicy | | | | | | | | | | | lava 🛛 🖸 Car | col <table-cell> S</table-cell> | iave and | lopis |
| Rulas Targeta (1) Security Intelligence HTTP Responses Advanced | | | | | | | | | | | | | | |
| 🏥 Filer by Derice | | | | | | | | | Q AH CI | legery 🤤 Add Rate | Search Rales | | | × |
| e Name | Searce Zenes | Deat Zones | Searce Networks | Deal Natworks | VLAN Tage | Users | Applications | See Parts | Deat Parts | URLa | Action | | | |
| Astenia intrator Balas | | | | | | | | | | | | | | |
| This category is empty | | | | | | | | | | | | | | |
| Standard Rales | | | | | | | | | | | | | | |
| 1 Dropf/DR0 | 40y | any | any . | # 172.16.32.1 | WV. | 101 | any . | any. | P BITP | 102 | 💢 Black | 0.01 | 3 D | / 8 |
| Roat Rules | | | | | | | | | | | | | | |
| We category a empty | | | | | | | | | | | | | | |
| Defeall Adam | | | | | | | | | Brirvalure | Prevention: Datascent Deca | By and Carried | vily | | |

Al het andere verkeer is geaccepteerd.

ISE-servicemodule voor vernieuwing

De huidige versie van de ISE-module die op het communautaire portaal wordt gedeeld, is *ISE 1.2 Remediation Bèta 1.3.19*:



This community supported remediation module allows for the automated interaction with Cisco Identity Services Engine (ISE) version 1.2. This interaction performs a quarantine of the desired IP (Source or Destination) based on the user configuration of the remediation. This quarantine action can be triggered by any event that occurs on the Sourcefre Defense Center that contains a source or destination IP address.

Navigeren in op **beleid > Handelingen > Verstellingen > Modules** en installeren het bestand:

| Overview Analysis Policies Devices Objects A | AMP | | | | |
|--|--------------------------|--|-------------------------|-----------------------------|---|
| Access Control Intrusion • Files Network Discovery | SSL Application Detector | irs Users | Correlation | Actions + Modules | |
| | | | | | |
| | | | | | , |
| | | | Success Module succe | esfully installed | |
| | | | Product Second | astany matanea | |
| Installed Remediation Modules | | | | | |
| Module Name | Version | Description | | | |
| Cisco IOS Null Route | 1.0 | Block an IP a | ddress in a Cisco IO | 05 router | |
| Cisco PIX Shun | 1.1 | Shun an IP address in the PIX firewall | | | |
| ISE 1.2 Remediation | 1.3.19 | Quarantine IF | addresses using 1 | dentity Services Engine 1.2 | |
| Nmap Remediation | 2.0 | Perform an N | map Scan | | |
| Set Attribute Value | 1.0 | Set an Attribu | ste Value | | |

Het juiste voorbeeld moet dan worden gecreëerd. Navigeer naar **beleid > Maatregelen > Remediations > Instanties** en verstrek het IP-adres van het beleidsbeheerknooppunt (PAN), samen met de ISE-administratieve aanmeldingsgegevens die nodig zijn voor REST API (een afzonderlijke gebruiker met de *ERS Admin*-rol wordt aanbevolen):

| Edit Instance | |
|--|-------------------------------|
| Instance Name | ise-instance |
| Module | ISE 1.2 Remediation (v1.3.19) |
| Description | |
| Primary Admin Node IP | 172.16.31.202 |
| Secondary Admin Node IP (optional) | |
| Username | admin |
| Password Retype to confirm | ••••• |
| SYSLOG Logging | 💿 On 🔵 Off |
| White List (an <i>optional</i> list of networks) | |
| | Create Cancel |

Het IP-adres van de bron (aanvaller) moet ook worden gebruikt voor herstel:

| Configured Remediations | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|
| Remediation Name Remediation Type Description | | | | | | | | | |
| No configured remediations available | | | | | | | | | |
| Add a new remediation of type Quarantine Source IP V Add | | | | | | | | | |

Correlatiebeleid

U moet nu een specifieke correlatieregel configureren. Deze regel wordt geactiveerd aan het begin van de verbinding die de eerder gevormde toegangscontroleregel (*DropTCP80*) aanpast. Om de regel te configureren volgt u **beleid > Correlatie > Regelbeheer**:

| Overview | Analysis | Policies | Devices O | bjects Al | MP | | | | |
|---------------|--------------|----------------|------------------|-----------------|-------------|---------------------------|------------------|-------------------|-----------|
| Access Contro | l Intru | sion • Fil | es Network | Discovery | SSL | Application Detecto | rs Users | Correlation | Actions 🔻 |
| | | | | | | | | | |
| Policy Ma | nagement | Rule M | anagement | White Lis | st Tr | affic Profiles | | | |
| Rule Info | rmation | | | | | | | | |
| Rule Name | | CorrelateTCP | 80Block | | | | | | |
| Rule Descrip | ption | | | | | | | | |
| Rule Group | | Ungrouped | V | | | | | | |
| Select th | ie type of | event for | this rule | | | | | | |
| If a cont | nection even | t occurs 🗸 | at the beginning | of the connect | tion | ✓ and if | meets the fo | llowing condition | ns: |
| | O Add co | ondition | Add complex | condition | | | | | |
| | × Acce | ss Control Rui | e Name 🗸 🗸 | contains the | e string 🔻 | DropTCP80 | | | |
| | | | | | | | | | |
| Rule Opt | ions | | | | | | | | |
| Snooze | | If this rule g | enerates an even | t, snooze for 0 | hou | rs v | | | |
| Inactive Peri | iods | There are no | defined inactive | periods. To ad | id an inaci | tive period, click "Add I | nactive Period". | | |
| | | | | | | | | | |
| | | | | | | | | | |

Deze regel wordt gebruikt in het Correlatiebeleid. Navigeer naar **beleid > Correlatie > Beleidsbeheer** om een nieuw beleid te creëren en voeg dan de geconfigureerde regel toe. Klik op **Opfrissen** aan de rechterkant en voeg twee handelingen toe: **sanering voor sourceIP** (eerder geconfigureerd) en **syslog**:

| Overview Analysis 🍺 | vervleiv Analysis Politices Devices Objects AHP 🔹 ederale v | | | | | | | | | | |
|---|--|--|--|--------------|------------|--|--|--|--|--|--|
| Polics Henegement | Pees Network Decovery Sol. Application Detectors U Polie Management White List Traffic Profiles | ant Cerreston Attaver | | Arts Version | 071 SF3454 | | | | | | |
| Correlation Policy 3rt Policy Name Policy Description | ormatiki n Conclui odhika | | | i dena i | 62900 | | | | | | |
| Policy Rules | Dec.× | Bargarana | | Q. Praty | Ado Ruita | | | | | | |
| Correlete 762908lock | | mysiling (Dyning) Sourcedtrifestmettindent premiedenticity | | Drint v | 40 | | | | | | |
| | | Responses for ContrelaterCPADBlock Assigned Responses Unascipted Responses Unascipted Responses Unascipted Responses | | | | | | | | | |

Zorg ervoor dat u het correlatiebeleid mogelijk maakt:



ASA

Een ASA die als VPN-gateway fungeert, wordt ingesteld om ISE voor verificatie te gebruiken. Het is ook noodzakelijk om de boekhouding en de RADIUS-CoA mogelijk te maken:

```
tunnel-group SSLVPN-FIRESIGHT general-attributes
address-pool POOL-VPN
authentication-server-group ISE
accounting-server-group ISE
default-group-policy POLICY
aaa-server ISE protocol radius
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
key ****
webvpn
enable outside
enable inside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable
```

ISE

Netwerktoegangsapparaat (NAD) configureren

Navigeer naar Beheer > Netwerkapparaten en voeg de ASA toe die als een RADIUS-client werkt.

Adaptieve netwerkcontrole inschakelen

Navigeer naar **Beheer > Systeem > Instellingen > Adaptieve Netwerkcontrole** om quarantaine API en functionaliteit mogelijk te maken:



Opmerking: In versies 1.3 en eerder wordt deze optie Endpoint Protection Service genoemd.

Quarantine DACL

Als u een DACL-toegangscontrolelijst (Downloadable Access Control List) wilt maken die voor de in quarantaine geplaatste hosts wordt gebruikt, navigeer dan naar **Policy > Resultaten > Automation > Downloadbare ACL**.

Licentieprofiel voor Quarantine

Navigeren in naar **beleid > Resultaten > Vergunning > Vergunningsprofiel** en maken een autorisatieprofiel met de nieuwe DACL:

| cisco Identity Services Engine | 1 | Home | Operations 🔻 | Policy V | Guest Access |
|------------------------------------|---|----------------------------------|------------------|------------|--------------|
| 💄 Authentication 🛛 💿 Authorization | 💦 Profiling 🛛 💽 P | osture | 💫 Client Provi | sioning | 🚊 TrustSec |
| Dictionaries Conditions Results | | | | | |
| Results | Authorization Prof Authorization * Name Description * Access Type Service Template | iles > Lim Profile Limited | Access Access | <u>,</u> | |
| Client Provisioning | ▼ Common Ta | sks | | | |
| TrustSec | DACL Name | | DE | NY_ALL_QU/ | ARANTINE 🍷 |

machtigingsregels

U moet twee vergunningsregels opstellen. De eerste regel (ASA-VPN) verleent volledige toegang voor alle VPN sessies die op de ASA worden beëindigd. De regel *ASA-VPN_quarantaine* wordt ingedrukt voor de opnieuw geauthentiseerde VPN sessie wanneer de host al in quarantaine is geplaatst (de beperkte toegang tot het netwerk wordt verleend).

Om deze regels te maken, navigeer dan naar Beleids > Vergunning:

| ahaha | | | | | | | | | | | | |
|---|------------------------------|------------------|-----------------------|---------------------------------------|-------------|--------------|------|---------------|--|--|--|--|
| cisco Ide | entity Services Engine | | 🟠 Home | Operations • | Policy 🔻 | Guest Access | Ac | dministration | | | | |
| 💄 Authenti | ation 🧕 Authorization | Ref Profiling | 💽 Posture | 🛃 Client Provi | sioning | 📑 TrustSec | 🐥 Po | licy Elements | | | | |
| Authorization Policy | | | | | | | | | | | | |
| Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. | | | | | | | | | | | | |
| For Poincy Export go to Administration > System > backup & Restore > Poincy Export Fage | | | | | | | | | | | | |
| First Matche | First Matched Rule Applies * | | | | | | | | | | | |
| Exception | s (0) | | | | | | | | | | | |
| Standard | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| Status | Rule Name | Cond | ditions (identity gro | ups and other con- | ditions) | | | Permissions | | | | |
| | ASA-VPN_quarantine | if (DEV Sessi | ICE:Device Type E | QUALS All Device JALS Quarantine) | Types#ASA- | VPN AND | then | LimitedAccess | | | | |
| | ASA-VPN | if DEV | CE:Device Type E | QUALS All Device | Types#ASA-V | PN | then | PermitAccess | | | | |

Verifiëren

Gebruik de informatie in deze sectie om te controleren of uw configuratie correct werkt.

AnyConnect start ASA VPN-sessie

| 🕥 Cisco AnyCo | nnect Secure Mobility Client | - • • |
|---------------|--|------------------|
| | VPN: Connected to 172.16.31.100. 172.16.31.100 | Disconnect |
| 00:00:09 | | IPv4 |
| ۞ (i) | | altalta cisco |

ASA creëert de sessie zonder DACL (volledige netwerktoegang):



Index : 37 Public IP : 192.168.10.21 : cisco Username Assigned IP : 172.16.50.50 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Essentials Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 18706 Bytes Rx : 14619 Tunnel Group : SSLVPN-FIRESIGHT Group Policy : POLICY Login Time : 03:03:17 UTC Wed May 20 2015 : 0h:01m:12s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : ac10206400025000555bf975 Security Grp : none

DTLS-Tunnel: <some output omitted for clarity>

Toegang tot gebruikerspogingen

Zodra de gebruiker probeert om toegang tot http://172.16.32.1 te krijgen, wordt het toegangsbeleid gevolgd, wordt het verkeer dat correspondeert online geblokkeerd en wordt het syslogbericht verzonden vanaf het FirePower Management IP-adres:

May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine (cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User: Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown, Access Control Rule Name: DropTCP80, Access Control Rule Action: Block, Access Control Rule Reasons: Unknown, URL Category: Unknown, URL Reputation: Risk unknown, URL: Unknown, Interface Ingress: eth1, Interface Egress: eth2, Security Zone Ingress: Internal, Security Zone Egress: External, Security Intelligence Matching IP: None, Security Intelligence Category: None, Client Version: (null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0, NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes: 66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A, SSL Subject CN: N/A, SSL Subject Country: N/A, SSL Subject OU: N/A, SSL Subject Org: N/A, SSL Issuer CN: N/A, SSL Issuer Country: N/A, SSL Issuer OU: N/A, SSL Issuer Org: N/A, SSL Valid Start Date: N/A, SSL Valid End Date: N/A, SSL Version: N/A, SSL Server Certificate Status: N/A, SSL Actual Action: N/A, SSL Expected Action: N/A, SSL Server Name: (null), SSL URL Category: N/A, SSL Session ID:

FireSight Correlatie Policy Sit

Het FireSight Management (Defense Center) Correlatiebeleid is aangetast, wat wordt gemeld door het syslog-bericht dat vanuit Defense Center wordt verstuurd:

May 24 09:37:10 **172.16.31.206** SFIMS: **correlation Event**: **correlateTCP80Block/CorrelationPolicy** at Sun May 24 09:37:10 2015 UTCConnection Type: FireSIGHT **172.16.50.50:49415 (unknown)** -> **172.16.32.1:80 (unknown)** (tcp) In dit stadium gebruikt het Defense Center de REST API (quarantaine)-oproep naar ISE, een HTTPS-sessie, die kan worden gedecrypteerd in Wireshark (met de Secure Socket Layer (SSL) plug-in en de privé-sleutel van het PAN-bestuurlijke certificaat):

| 120 172 | 2,16,31,206 | 172.16.31.202 | LSv1 | 583 Client Hello | | | | | | | |
|---|--|-------------------|-------------------|---|--|--|--|--|--|--|--|
| 121 173 | 2.16.31.202 | 172,16,31,206 | TCP | 66 https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165857 TSecr=97280105 | | | | | | | |
| 122 173 | 2.16.31.202 | 172.16.31.206 | TCP | 952 [TCP segment of a reassembled PDU] | | | | | | | |
| 123 173 | 2.16.31.202 | 172.16.31.206 | T_Sv1 | 681 Server Hello, Certificate, Certificate Request, Server Hello Done | | | | | | | |
| 124 173 | 2.16.31.206 | 172.16.31.202 | TCP | 66 48046 > https [ACK] Seq=518 Ack=1449 Win=17536 Len=0 TSval=97280106 TSecr=389165957 | | | | | | | |
| 125 17 | 2.16.31.206 | 172.16.31.202 | TCP | 66 48046 > https [ACK] Seq=518 Ack=2897 Win=20480 Len=0 TSval=97280106 TSecr=389165957 | | | | | | | |
| 126 17 | 2.16.31.206 | 172.16.31.202 | TCP | 66 48046 > https [ACK] Seq=518 Ack=3512 Win=23296 Len=0 TSval=97280106 TSecr=389165958 | | | | | | | |
| 127 173 | 2.16.31.206 | 172.16.31.202 | T_Sv1 | 404 Certificate, Client Key Exchange, Change Cipher Spec, Finished | | | | | | | |
| 128 172 | 2.16.31.202 | 172.16.31.206 | T_Sv1 | 72 Change Cipher Spec | | | | | | | |
| 129 17 | 2.16.31.202 | 172.16.31.206 | TLSv1 | 119 Finished | | | | | | | |
| 130 172 | 2.16.31.206 | 172.16.31.202 | TCP | 66 48046 > https [ACK] Seq=856 Ack=3571 Win=23296 Len=0 TSval=97280107 TSecr=389165962 | | | | | | | |
| 131 17 | 2.16.31.206 | 172.16.31.202 | HITP | 295 GET /ise/eps/QuarantineByTP/172.16.50.50 HTTP/1.1 | | | | | | | |
| 132 173 | 2.16.31.202 | 172.16.31.206 | TCP | 66 https > 48046 [ACK] Seq=3571 Ack=1085 Win=17792 Len=0 TSval=389166020 TSecr=97280111 | | | | | | | |
| 135 173 | 2.16.31.202 | 172.16.31.206 | HTTP/XML | 423 HTTP/1.1 200 OK | | | | | | | |
| r Cartina Co | zon concrot - | 10100017 010 101 | CT 10/0 10 1 10/0 | ary and there include that y deale and ment and the contraction | | | | | | | |
| ~ 0.001 C 0.0 | - SCUIE SUCKEIS Layer - T Oct Beneral Leven | | | | | | | | | | |
| Capte | etti Tyney Appl | ication Data /22/ | Y FIOLOGICE THE | h. | | | | | | | |
| Versi | $m \in T \mid S = 1 \land A$ | nya201) | <i>,</i> | | | | | | | | |
| Lengt | bi 224 | 040301) | | | | | | | | | |
| Eacry | nted Applicati | ion Data: elde29 | faa3cef63e99d | 97#0#9F9Fd401c9dd1cd117cb7#9 | | | | | | | |
| - Hypertext | Transfer Pro | tecel | 199966-1996999 | | | | | | | | |
| Appendexe CET / is | e/ens/fuarant | ineByIE/172_16_51 | 0 50 HTTP/1 1 | r\n | | | | | | | |
| TE: def | late.gzip:g=0 | .3\r\n | | · • | | | | | | | |
| Connect | ion: TE, clas | e\r\n | | | | | | | | | |
| ▷ Authori | zation: Basic | WRtaw46S3Cha29 | 3MTIz\r\n | | | | | | | | |
| Host: 1 | 72.16.31.202 | r\n | | | | | | | | | |
| User-Ap | ent: libww-p | er1/6.06\r\n | | | | | | | | | |
| \r\n | | | | | | | | | | | |
| IBULL r | equest URI: h | ttp://172.16.31.0 | 202/1se/eps/0 | arantineBvIP/172.16.50.501 | | | | | | | |
| | | | and and shart a | | | | | | | | |

In GET is het verzoek om het IP-adres van de aanvaller doorgegeven (172.16.50.50) en die host wordt in quarantaine geplaatst door de ISE.

Navigeer naar Analyse > Correlatie > Status om het succesvolle herstel te bevestigen:

| Overview Analysis Policies Devices Objects AMP | | | | | | | | | | | | |
|--|------------------|-------------------|---------|--------------|---------|-------------------|----------------------|----------|----------------------|--------------------------------------|--|--|
| Context Explorer | Connections • | Intrusions • | Files # | Hosts • | Users • | Vulnerabilities • | Correlation + Status | Custom • | Search | | | |
| | | | | | | | | | | Bookmark This Page | | |
| Remediation Status | | | | | | | | | | | | |
| No Search Constraints (<u>Hith Search</u>) | | | | | | | | | | | | |
| Jump to * | Jump to * | | | | | | | | | | | |
| Time × | | | Ret | mediation N | ame × | | Palley × | | Rule × | Result Message X | | |
| 4 📃 2015-05 | -24 10:55:37 | | 500 | tor3P-Remedi | lation | | Correlation Policy | | Cornelated CP80Block | Successful completion of remediation | | |
| 4 📃 2015-05 | -24.10:47:08 | | 500 | rcelP-Remeti | ation | | Correlation Policy | | CorrelateFCP90Block | Successful completion of remediation | | |
| IC < Page 1 of 1 | >>> Displaying r | ows 1-2 of 2 rows | | | | | | | | | | |
| View | Delete | | | | | | | | | | | |
| View At | Delete All | | | | | | | | | | | |

ISE voert quarantaine uit en zendt CoA toe

In dit stadium deelt ISE prrt-management.log mee dat de CoA moet worden verstuurd:

Met behulp van een opdrachtregel (prt-server.log) wordt het bericht van CoA naar de NAD verstuurd, dat de sessie (ASA) beëindigt:

INFO [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -:::::- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault

Wanneer u navigeert naar **Operations > Verificatie**, dient u te tonen dat *Dynamische autorisatie is gelukt*.

VPN-sessie is losgekoppeld

De eindgebruiker stuurt een kennisgeving om aan te geven dat de sessie losgekoppeld is (dit proces is transparant voor 802.1x/MAB/gast bedraad/wireless):



Details uit de Cisco AnyConnect-logbestanden tonen:

10:48:05 AM Establishing VPN... 10:48:05 AM Connected to 172.16.31.100. 10:48:20 AM Disconnect in progress, please wait... 10:51:20 AM The secure gateway has terminated the VPN connection. The following message was received from the secure gateway: COA initiated

VPN-sessie met beperkte toegang (quarantaine)

Omdat altijd-on VPN is geconfigureerd wordt de nieuwe sessie onmiddellijk gebouwd. Dit keer

wordt de ISE ASA-VPN_quarantaineregel geraakt, die de beperkte netwerktoegang verleent:

| 🛛 👪 Author | ntications | 👖 Rep | orta | Adaptive | Network Central | 💊 Troubleshoot | | | | |
|--|--------------|-----------------|---------|----------|-----------------|----------------------|--|------------------------|---------------------------------|--|
| | Misconfigure | d Supple | cants 🤇 | Ð | Miscon | figured Network Devi | ces @ | ADIUS Drops @ | Client Stopped | |
| | 0 | | | | 0 | | 0 | 0 | | |
| | | | | | | | | | | |
| 🖬 Show Live Sessions 🙀 Add or Remove Columns 🔻 🧁 Refresh 👔 Reset Repeat Counts 🛛 😵 Refresh 👔 Refresh 😨 Reset Repeat Counts | | | | | | | | | | |
| Time | • | Status Ali 👻 | Det | Repeat C | Identity D | Endpoint ID | Authorization Policy | Authorization Profiles | Event ① | |
| 2015-05-2 | 410:51:40 | 0 | 6 | 0 | cisco | 192,169,10,21 | | | Session State Is Started | |
| 2015-05-2 | 410:51:35 | | ò | | #ACSACL#+P4 | D | | | DACL Download Succeeded | |
| 2015-05-2 | 410:51:35 | - - | ò | | cisco | 192,169,10,21 | ${\tt Default} >> {\tt ASA-VPN}_quarantine$ | UmitedAccess | Authentication succeeded | |
| 2015-05-2 | 410:51:17 | 1 | ò | | | 08:00:27:0A:EP:AD | | | Dynamic Authorization succeeded | |
| 2015-05-2 | 410:48:01 | - - | ò | | cisco | 192,168,10,21 | Default >> ASA-VPN | PermitAccess | Authentication succeeded | |

Opmerking: De DACL wordt gedownload in een afzonderlijk RADIUS-verzoek.

Een sessie met beperkte toegang kan op de ASA met de **show vpn-sessiondb detail** worden geverifieerd **in elke connect** CLI-opdracht:

asav# show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
```

Username : cisco Index : 39 Assigned IP : 172.16.50.50 Public IP : 192.168.10.21 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Essentials Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 : 11436 : 8 Bytes Tx Bytes Rx : 4084 Pkts Tx : 8 Pkts Rx : 36 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : POLICY Tunnel Group : SSLVPN-FIRESIGHT Login Time : 03:43:36 UTC Wed May 20 2015 : 0h:00m:10s Duration Inactivity : 0h:00m:00s VLAN : none VLAN Mapping : N/A Audt Sess ID : ac10206400027000555c02e8 Security Grp : none DTLS-Tunnel: <some output ommited for clarity> Filter Name : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

FireSight (defensiecentrum)

Het ISE-herstelscript bevindt zich op deze locatie:

lib ise-instance ise-test.pl **ise.pl** module.template

Dit is een eenvoudig *perl* script dat het standaard SourceFire (SF) logging subsysteem gebruikt. Nadat het herstel is uitgevoerd, kunt u de resultaten bevestigen via de */var/log/berichten*:

```
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) 172.16.31.202 - Success 200 OK - Quarantined
172.16.50.50 as admin
```

ISE

Het is belangrijk dat u de Adaptieve Network Control Service op ISE instelt. Om de gedetailleerde logbestanden in een run-proces te bekijken (*prt-management.log* en *prt-server.log*) moet u het DEBUG-niveau inschakelen voor de Runtime-AAA. Navigeer naar Administratie > Systeem > Vastlegging > Logconfiguratie > Debug Log configuratie om de knoppen in te schakelen.

U kunt ook navigeren naar **Operations > Rapporten > Endpoint en gebruikers > Adaptieve audit van netwerkcontrole** om informatie te bekijken voor elke poging en resultaat van een quarantaineverzoek:

| cisco Identity Services Engine | 🕥 Hot | Bit Operations • | Policy V Ga | ent Access V | Administration | | | |
|--|------------------------------------|-----------------------|--------------|--------------|----------------|--------------|---------------------|---------------|
| authenblastons 📑 Reports 🔯 Adaptive Network Control 💊 Troubleshoot | | | | | | | | |
| Report Selector Adaptive Network Control Audit | | | | | | | | |
| Favorites | | | | | | | | |
| ISE Reports | From 05/24/2015 12:00:0 | 0 AM to 05/24/2015 09 | 3621 PM | | | | | |
| Auth Services Status B reports | Logged At 2015-05-24 21-30-32 3 | Endpoint ID | IP Address | Operation | Operation | Operation ID | Audit Session Admin | Admin IP |
| Deployment Status 12 reports | 2015-05-24 21:30:32.3 | 192.168.10.21 | 172.16.50.50 | Quarantine | RUNNING | 512 | ac1020640003 admin | 172.16.31.206 |
| + Endpoints and Users | 2015-05-24 21:29:47.5 | 08:00:27:DA-EF-A | | Unquarantine | SUCCESS | 507 | ec1020640005 | |
| Client Provisioning | 2015-05-24 21:29:47.4 | 08:00:27:DA-EF-A | | Unquarantine | RUNNING | 507 | ac1020640005 admin | 172.16.31.202 |
| Current Active Sessions | 2015-05-24 21:18:25.2 | 08:00:27:DA:EF:A | | Quarantine | FALURE | 480 | ac1020640005 | |
| Adaptive Network Control Aude | 2015-05-24 21:18:25.2 | 08:00:27:04:EF:A | | Quarantine | RUNNING | 480 | ac1020640005 admin | 172.16.31.202 |
| V Alters - | 2015-05-24 21:11:19.8 | 08:00:27:DA:EF:A | | Unquarantine | SUCCESS | 471 | ac1020640005 | |
| * Time Range Today * | 2015-05-24 21:11:19.8 | 08:00:27:0A:EF-A | | Unquarantine | RUNNING | 471 | ac1020640005 admin | 172.16.31.202 |
| But | 2015-05-24 21:10:13:5 | 192.168.10.21 | 172.16.50.50 | Unquarantine | SUCCESS | 462 | ac1020640005 | |
| | 2015-05-24 21:10:13.5 | 192.168.10.21 | 172.16.50.50 | Unquarantine | RUNNING | 462 | ac1020640005 admin | 172.16.31.202 |
| External Mobile Device Management | 2015-05-24 18:05:10.7 | 08:00:27:0A:EF:A | | Quarantine | SUCCESS | 337 | ac1020640005 | |
| Posture Detail Assessment | 2015-05-24 18:05:10.7 | 08:00:27:0A-EF-A | | Quarantine | RUNNING | 337 | ac1020640005 admin | 172.16.31.202 |
| Profiled Endpoints Summary | 2015-05-24 18:00:05.4 | 192.168.10.21 | 172.16.50.50 | Quarantine | SUCCESS | 330 | ac1020640005 | |
| Endpoint Profile Changes | 2015-05-24 18:00:05.4 | 192.168.10.21 | 172.16.50.50 | Quarantine | RUNNING | 330 | ac1020640005 admin | 172.16.31.206 |
| Top Authorizations by Endpoint | 2015-05-24 13:40:56.4 | 192.168.10.21 | 172.16.50.50 | Quarantine | SUCCESS | 291 | ac1020640005 | |
| The Advantations builded | 2015-05-24 13:40:56.4 | 192.168.10.21 | 172.16.50.50 | Quarantine | RUNNING | 291 | ac1020640005 admin | 172.16.31.206 |
| Top Authorizations by User | 2015-05-24 11:37:29.3 | 192.168.10.21 | 172.16.50.50 | Quarantine | SUCCESS | 250 | ac1020640005 | |
| User Change Password Audit | 2015-05-24 11:37:29.3 | 192.168.10.21 | 172.16.50.50 | Quarantine | RUNNING | 250 | ac1020640005 admin | 172.16.31.206 |
| Supplicant Provisioning | 2015-05-24 10:55:55.8 | 192.168.10.21 | 172.16.50.50 | Quarantine | SUCCESS | 207 | ac1020640005 | |
| Registered Endpoints | 2015-05-24 10:55:55.8 | 192.168.10.21 | 172.16.50.50 | Quarantine | RUNNING | 207 | ac1020640005 admin | 172.16.31.206 |
| Endpoints Purge Activities | 2015-05-24 10:55:29.7 | 08:00:27:DA-EF-A | | Unquarantine | SUCCESS | 206 | ac1020640005 | |
| Guest Access Reports Sizeonts | 2015-05-24 10:55:29.7 | 08:00:27:DA:EF:A | | Unquarantine | RUNNING | 206 | ac1020640005 admin | 172.16.31.202 |
| | 2015-05-24 10:51:17.2 | 08:00:27:0A-EF-A | | Quarantine | SUCCESS | 189 | ac1020640005 | |
| Saved and Scheduled Reports | 2015-05-24 10:51:17.2 | 00.00.17.04.EE.K | | Automation | RUNNING | 189 | ar1020640005 admin | 1721631202 |

Bugs

Raadpleeg Cisco bug-ID <u>CSCu41058</u> (ISE 1.4 Endpoint Quarantine inconsistentie en VPNstoring) voor informatie over een ISE-bug die is gerelateerd aan VPN-sessies (prima werkt 802.1x/MAB).

Gerelateerde informatie

٠

- ISE versie 1.3 pxGrid-integratie met IPS PxLog toepassing
- Administrator Guide van Cisco Identity Services Engine, release 1.4 adaptieve netwerkcontrole instellen
- <u>Referentiegids voor Cisco Identity Services Engine API, release 1.2 Inleiding naar API voor</u> boekingen met externe REST-services
- <u>Cisco Identity Services Engine API Referentiegids, release 1.2 Inleiding naar de BEWAKING REST API's</u>
- Administrator-gids voor Cisco Identity Services Engine, release 1.3
- Technische ondersteuning en documentatie Cisco-systemen