

مادختساب pxGrid Firepower 6.1 ةجلاعم نيوكت ISE

تايوتحمل

[ةمدقمل](#)

[ةيساسأل تابلطتم](#)

[تابلطتم](#)

[ةمدختسمل تانوكمل](#)

[نيوكتل](#)

[ةكبش لل يطيطختل مسرل](#)

[Firepower نيوكت](#)

[ISE نيوكت](#)

[ةحصل نم ققحتل](#)

[اهالصل او ااطخال فاشكتسا](#)

[ةلصل تاذ تامولعم](#)

ةمدقمل

ةيوهل تامدخ كرحم مادختساب pxGrid Firepower 6.1 ل نيوكت ةيفي دننتسمل اذه حضوي (ISE) ةياهن ةطقن ةيامح ةمدخ عم 6.1+ ISE Firepower ةجلاعم ةدحو مادختسا نكمي. (ISE) ةكبش لل لوصول ةقبط ل ع نيجمجاهم لل ءادوس لل ةمئاقل/ةقاطب لل ةتمأل

ةيساسأل تابلطتم

تابلطتم

ةيلال عيضاوملاب ةيساسأ ةفرعم كي دل نوكت نأب Cisco ي صوت

- Cisco ISE
- Cisco Firepower

ةمدختسمل تانوكمل

ةيلال ةيدامل تانوكمل او جماربلا تارادصل ل دننتسمل اذه يف ةدراول تامولعمل دننتست

- Cisco ISE، رادصلإا 2.0 Patch 4
- Cisco Firepower 6.1.0
- ةيرهاظلا ةيكلسالل LAN ةكبش يف مكحتل ةدحو (vWLC) 8.3.102.0

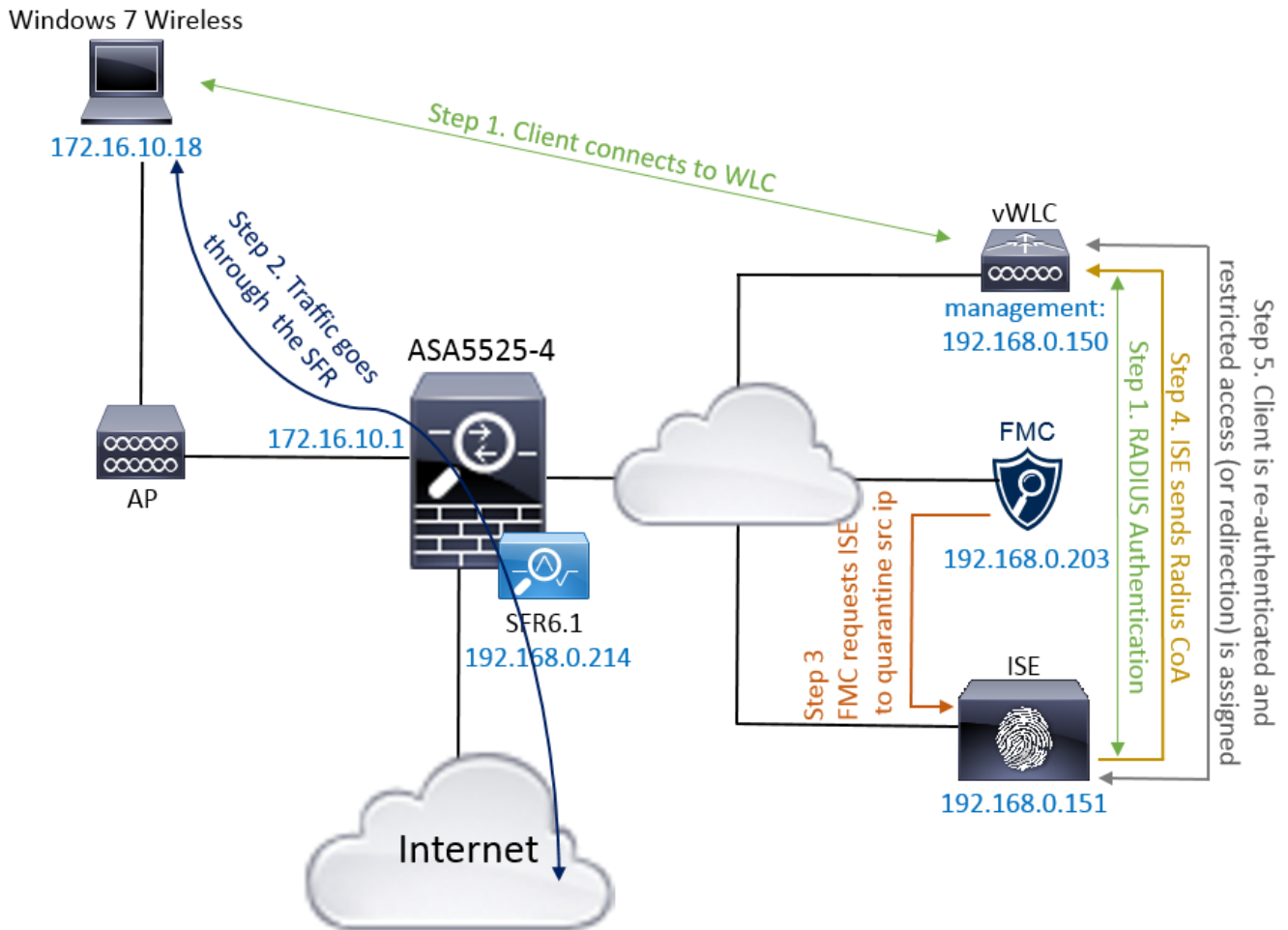
ةصاخ ةيلمعم ةئيب يف ةدوومل ةزهأل نم دننتسمل اذه يف ةدراول تامولعمل ءاشنإ مت تناك اذإ. (يضارفتفا) حوسم نيوكتب دننتسمل اذه يف ةمدختسمل ةزهأل عيجم تآب رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف، ةرشابم كتكبش

نيوكتل

Active Directory (AD) مع ISE لمكت و FirePOWER مع ISE لمكت ليلوالا نيوكتال ةلاقملا هذه يطغت ال ةدحو حمت. عجارملا مسق لىل لقتنا تامولعمل هذل. AD مع Firepower لمكت و (AD) ءاغلا، يحصلا روجل) ISE EPS تاي ناكم مادختساب FirePOWER ماطنل 6.1 Firepower حالصال طابترالا ةدعاق ةقباطم دنع جالعك (ذفنملا ليغشت فاقيا، يحصلا روجل

ةيكلساللا رشنلا تاي لمعل ذفنملا ليغشت فاقيا رفوتيا ال: ةظالم

ةكبشلال يطيختال مسرلا



قفتل فصول:

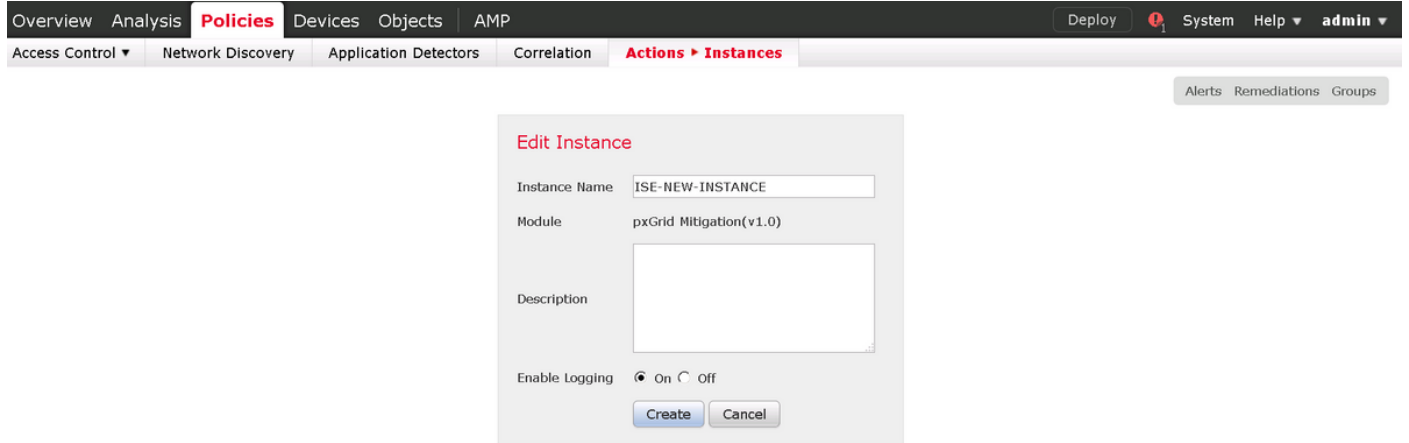
1. ليوخت فيرعت فللمب ليوخت ةدعاق لىل لخدو ISE عم قداصيو ةكبشبال لىمعل لصتيا. ةكبشلال لىل ديقم ريغ الوصوحنمي.
2. FirePOWER زاغ ربع لىمعل نم رورملا ةكرح قفتت مث.
3. ليغشتب اهروذب موقت طابترالا ةدعاق برضيو راض طاشن ذيفنت ي ف مدختسملا أدبي. PXgrid ربع ISE ءجالعمب مايقلل (FMC) FirePOWER ةرادا زكرم.
4. ريغت ليغشتب موقيو ةياهنلا ةطقن لىل EPSStatus لزعة لىمعل نىيعتب ISE موقيو (لوجل و WLC) ةكبشلال لىل لوصو زاغ لىل RADIUS ضيوفت.
5. SGT ريغت موقيو) اديقم الوصو نىيعت رخأ صيخرت ةسايس ذيفنتب لىمعل موقيو (لوصلو صفر و ةباوبل لىل هيجوتل ةدعاق و).

ةظالم ISE لىل RADIUS ةبساحم لاسرال (NAD) ةكبشلال لىل لوصولو زاغ نيوكت بجي: ةظالم ةياهن ةطقن لىل IP ناووع نىيعتل اهمادختس متي يتال IP ناووع تامولعمب هديوزتل.

Firepower نيوكت

pxGrid فيفخت لثم نيوكت 1. ةوطخال

حضورم وه امك PxGrid فيفخت لثم ةفاض او تالثم ال > تاءارج ال > تاسايس ال ال لقتنا ةروصل ال في



Overview Analysis **Policies** Devices Objects AMP Deploy System Help admin

Access Control Network Discovery Application Detectors Correlation **Actions ▶ Instances** Alerts Remediations Groups

Edit Instance

Instance Name: ISE-NEW-INSTANCE

Module: pxGrid Mitigation(v1.0)

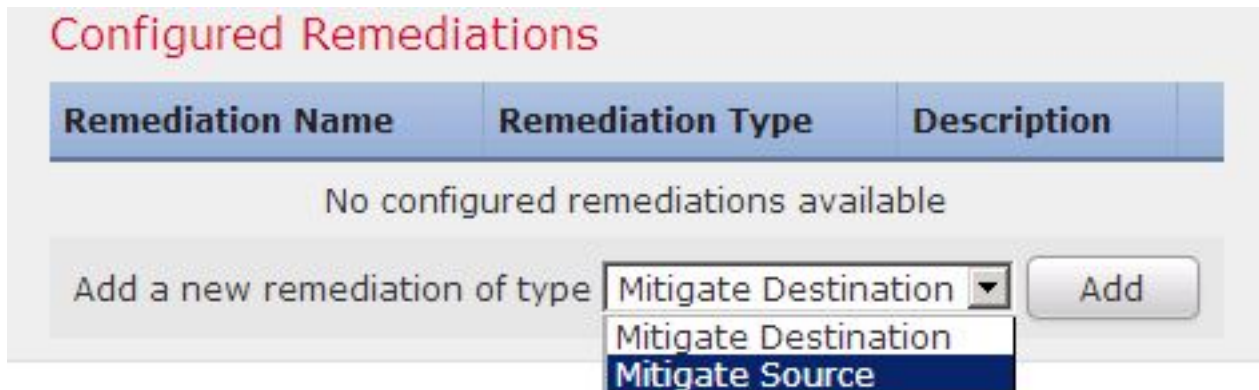
Description:

Enable Logging: On Off

Create Cancel

لح نيوكت 2. ةوطخال

فيفخت مادختسا م تي ، لالثلما اذه في . ردمصم ال نم دحل او ةهجولا فيفخت : نإحاتم نإعون كانه ةروصل ال في حضورم وه امك ةفاض رقناو ةجالعمل ال عون رتخأ . ردمصم ال



Configured Remediations

| Remediation Name | Remediation Type | Description |
|--------------------------------------|------------------|-------------|
| No configured remediations available | | |

Add a new remediation of type Mitigate Destination Mitigate Source Add

ةروصل ال في حضورم وه امك حالصل ال ال فيفخت ءارج نييعت

Edit Remediation

Remediation Name

Remediation Type

Mitigate Source

Description

Mitigation Action

Whitelist

(an optional list of networks)

Create

Cancel

طابترا ءءءاق نىوك ت 3 ءوطءال

وه ءءءاقلا طابترا ءءءاق ءاشن| قوف رقناو ءءءاقلا ءراء| > طابتراالا > تاساىسلا ىلا لقتنا اءه ىف . طورش ءء ىلع طابتراالا ءءءاق ىوتءء نأ نكم ى . ءالصالا ءىلمء لوصءل لغشملا ءءءولل IP ناوئء ناكو مءءءق| ءءء اذا PingDC طابتراالا ءءءاق ىلا لوصولا مءى ، لءءملا ىءص ىلع ءرلل ءقباطملا ءصصءملا لوصولا عنم ءءءاق نىوك مءى . 192.168.0.121 ءروصولا ىف ءصصوم وه امك رابءءءالا صرءل ICMP لوكوءورب :

The screenshot shows the 'Rule Management' section in Cisco ISE. The rule name is 'PingDC'. The rule description is empty. The rule group is 'Ungrouped'. The event type is 'an intrusion event occurs' and it meets the following conditions: 'Destination IP is 192.168.0.121'. There are buttons for 'Add Connection Tracker', 'Add User Qualification', and 'Add Host Profile Qualification'. Under 'Rule Options', there is a 'Snooze' field set to 0 hours and an 'Add Inactive Period' button.

طابت را جهن نيوك ت. 4 ةوطخل

ةفاضاب مقو ،ةسايس عاشن قوف رقن او ةسايس ال ةراد > طابت رال > تاسايس ال ال لقتنا ةروصل ال يف حضورم وه امك اهل ةباجتسال ال نيي عتب مقو ةسايس ال ال ةدع اق

The screenshot shows the 'Correlation Policy Information' section. The policy name is 'ise_corellation_policy'. The policy description is empty. The default priority is 'None'. There is a table for 'Policy Rules' with one entry: 'PingDC' with response 'QUARANTINE-SOURCE (Remediation)' and priority 'Default'. There are 'Save' and 'Cancel' buttons and an 'Add Rules' button.

ةروصل ال يف حضورم وه امك طابت رال ةسايس نيكم تب مق

The screenshot shows the 'Create Policy' button and a list of policies. The list has one entry: 'ise_corellation_policy'. There are 'Sort by' and 'State' dropdowns.

ISE نيوك ت

ل. ليوختل جهن نيوك ت. 1 ةوطخل

ارج دع اذهيفنت متيس ةديج ليوخت ةسايس فض او ضيوفتال > جهنل ال ال لقتنا نكمي يتل تاراخي ةدع كانه . طرشك لزع يواسي EPSStatus : ةسلج مادختسا . حالصال كذل ةجيتنك اهمادختسا

- ةزهجأ لىل لوصولو لىل ف م كحتلا دويق ضرف) ي مقرر دعاسم نيي عتو لوصولو اب حاسم لىل (ةكبشلا
- قمر لاصلتالا لىل ارداق نوكي نأ بجي الو ةكبشلا نم مدختسم لىل درط بجي) لوصولو ضرف (ىرخأ
- طاقنلا ةباوب نيوكت متي ،ويرانيسلا اذه يفي) ءادوس ةمئاق ةباوب لىل هي جوتلا ةداعإ لىل ضرغل اذهل ةصصخملا ةلاعفل

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|-------------------------------------|--------------------|---|-------------------------------------|
| <input checked="" type="checkbox"/> | AssignSGTBlockOnFP | if Session:EPSSStatus EQUALS Quarantine | then MaliciousUser AND PermitAccess |
| <input checked="" type="checkbox"/> | BlockOnISE | if Session:EPSSStatus EQUALS Quarantine | then DenyAccess |
| <input checked="" type="checkbox"/> | BlockOnISE_copy | if Session:EPSSStatus EQUALS Quarantine | then blacklist_redirect |

صصخملا لخدملا نيوكت

ةحفص طقف دجوت .ءادوس ةمئاقك ةنخاسلا طاقنلا ةباوب نيوكت مت ،لاثملا اذه يفي كلذ متي) AUP لوبقل ةينامك م دجوت الو صصخم صنب (AUP) ةلوبقم مادختسا ةسايس يفيخي زمر قصل م JavaScript نيكمت لىل الوا جاتحت ،كلذ قيقيحتل .(JavaScript مادختساب لخدملا صصخت نيوكت يفي م كحتلا رصانعو و AUP رز

لخدملا صصخت نيوكت يفي م كحتلا رصانعو و AUP رز

صصخت نيوكت يفي م كحتلا رصانعو و AUP رز

Portal Customization

Enable Portal Customization with HTML

Enable Portal Customization with HTML and JavaScript

Save

لاصلتالا ةطقن لخدم ءاشنإ .2 ةوطخل

قوف رقن او فيضلا تاباوب > (نيوكت) Configure > (فيضلا لوصولو) Guest Access لىل لقتنا ةلاعفل ةطقنلا عون رتخأ م ،(ءاشنإ) Create

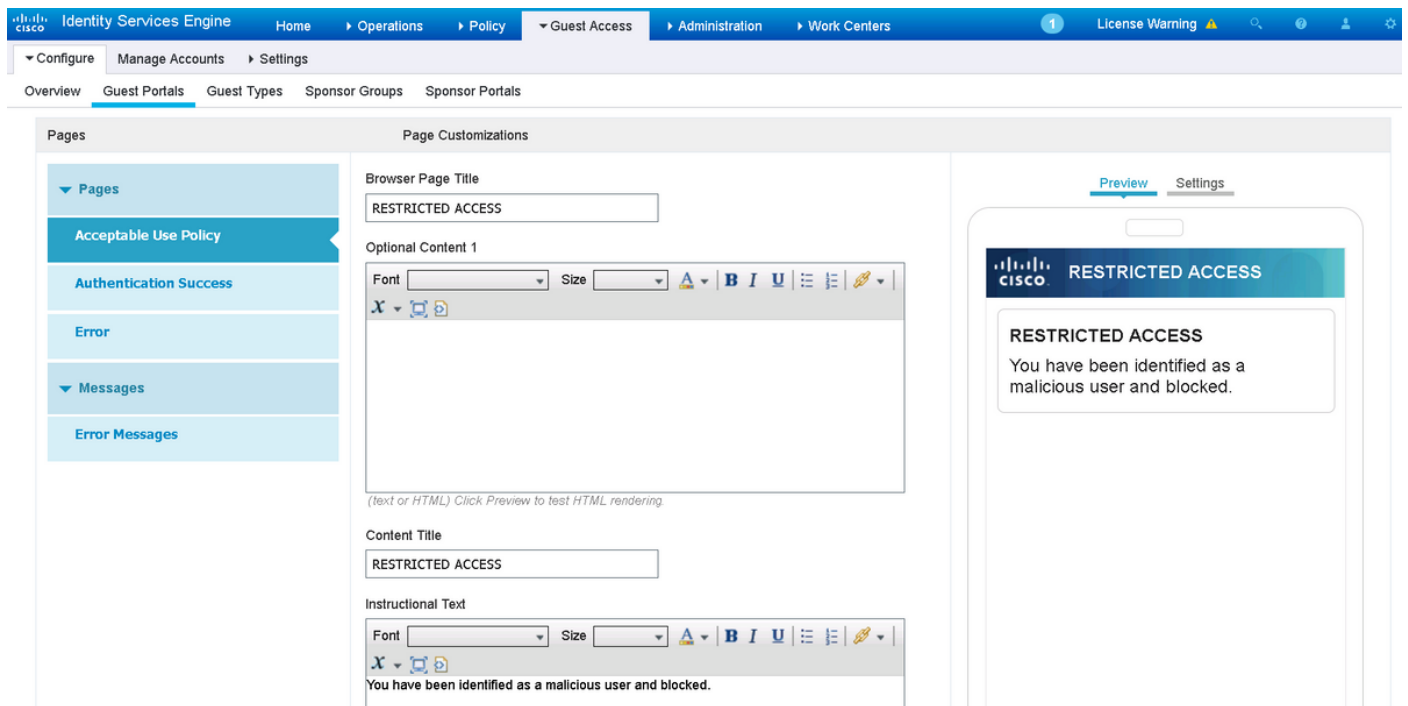
Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Create Edit Duplicate Delete

لخدمال صي صخت ني وكت 3 ةوطخل.

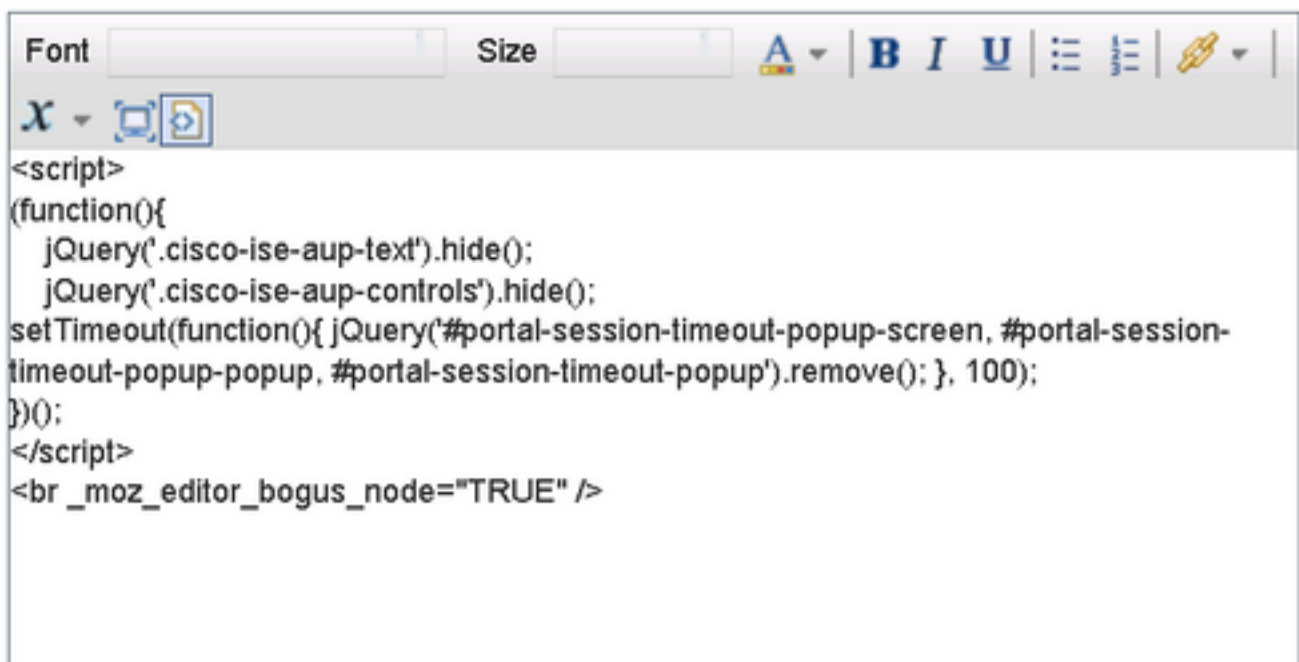
ريذحت ريفوتل يوتحمل او نيوانعل ريفيغت ب مقو لخدمال ةحفص صي صخت يلى لقتنا مدخت سملل بسانم.



يذيفنتال صنلا قصلب مقو، HTML رصم ليذبت رقنا 2، يوتحمل راخ يلى ريرمتلاب مق لخدال:

HTML رصم ليغشت اغل رقنا.

Optional Content 2



(text or HTML) Click Preview to test HTML rendering.

تحصيل نم ققحتلا

لكشب لمعي كيدل نيوكتلا نأ نم ققحتلل مسقلا اذه يف ةمدقملا تامولعمل مدختسأ
ححص.

نارينلا ةوق

Analysis لىلقنا . طابترالا ةدعاق / ةسايس نم برض وه حالصإلا ثودحل لغشملا
طابترالا ثدح ثودح نم ققحتو > Correlation > Correlation Events (لجحتلا)

| Time | Impact | Inline Result | Source IP | Source Country | Destination IP | Destination Country | Security Intelligence Category | Source User | Destination User | Source Port / ICMP Type | Destination Port / ICMP Code |
|---------------------|--------|---------------|--------------|----------------|----------------|---------------------|--------------------------------|-------------|------------------|-------------------------|------------------------------|
| 2017-02-16 13:27:51 | | | 172.16.10.19 | | 192.168.0.121 | | | | | 8 (Echo Request) / icmp | 0 / icmp |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

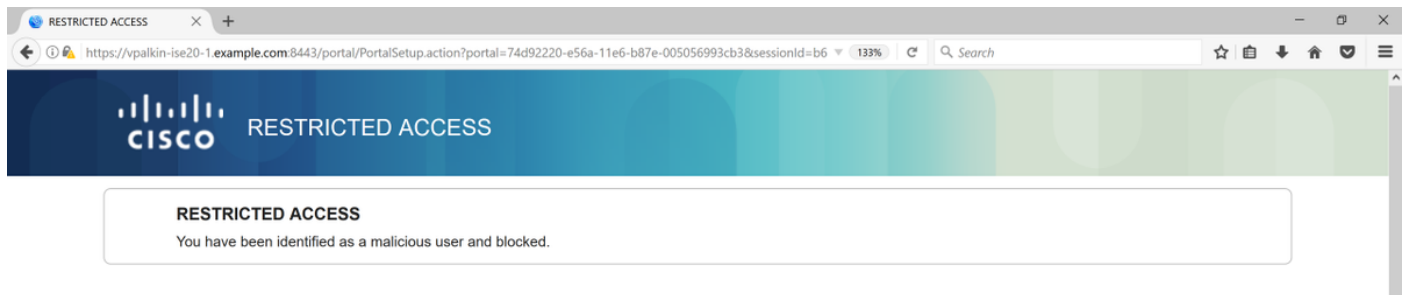
ةيوهلا فشك تامدخ كرحم (ISE)

نكميو ،مدختسمل ةقداصم ةداعاو RADIUS: CoA لىغشتب ISE موقى نأ بجى كلذ دعب
RADIUS livelog > ةيلعمل ايف ثادحالا هذه نم ققحتلا

| | | | | | | | | | |
|-------------------------|---|--|-------|-------------------|---------------------|-------------------------|--------------------------|----------------------------|------|
| 2017-02-16 13:26:22.894 | ✓ | | alice | E4:B3:18:69:EB:8C | Windows10-Workst... | Default >> Dot1X >> D.. | Default >> AssignSGT... | MaliciousUser,PermitAcc... | vWLC |
| 2017-02-16 13:26:21.040 | ✓ | | | E4:B3:18:69:EB:8C | | | | | vWLC |
| 2017-02-16 13:25:29.036 | ✓ | | alice | E4:B3:18:69:EB:8C | Windows10-Workst... | Default >> Dot1X >> D.. | Default >> Standard R... | PermitAccess,Administra... | vWLC |

ةلاح يف . ةياهنلا ةطقن لىلق فلتم Sgt MaliciousUser نىيىتبت ISE ماق ،لاثملا اذه يف
هنكمى الويكلساللا لاصتالا مدختسمل دق فى ،لوصولا لىوخت فىرعت فلم ضفر
ىرخا ةرم لاصتالا

ةداعال حالصإلا ضىوفت ةدعاق نيوكت مت اذا . ءادوسلا ةمئاقلا لخدم مادختساب حالصإلا
مجاهملا روظنم نم اذكه ودبت نأ بجى فى ، ةباوبلا لىلق هيجوتلا



اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمى تامولعمل مسقلا اذه رفوى

ةروصللا هذه يف حضورم وه امك (ةلاحلا) > Status > Correlation > Analysis (لجحتلا) لىلقنا

| Time | Remediation Name | Policy | Rule | Result Message |
|---------------------|-------------------|------------------------|--------|--------------------------------------|
| 2017-02-16 14:26:19 | QUARANTINE-SOURCE | ise_correlation_policy | PingDC | Successful completion of remediation |

syslog: ةني عم أطخ ةلسرر وأ حاجنب حالصإلا لامكإ اما ةجيتنلا ةلسرر عجرت نأ بجي
 يف تالجلسلا سفن نم ققحتلا نكمي. pxgrid عم جاتنإ حشرم و Syslog ةبقارم > ماظن
 /var/log/messages.

ةلص تاذا تامولعم

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html>
- <https://communities.cisco.com/docs/DOC-68284>
- <https://communities.cisco.com/docs/DOC-68285>
- <https://communities.cisco.com/thread/64870?start=0&tstart=0>
- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html
- <http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html>

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل