

Ø^ÙfÙ^ÙŠÙ† Ù^Ø¶Ø¹ÙŠØ© ISE Ø¹Ø·Ø± AnyConnect Remote Access VPN Ø¹Ù,,Ù% FTD

Ø§Ù,,Ù...ØØ^Ù^ÙŠØ§Ø^

- [Ø§Ù,,Ù...Ù,Ø-Ù...Ø©](#)
- [Ø§Ù,,Ù...Ø^Ø-Ù,,Ø·Ø§Ø^ Ø§Ù,,Ø£Ø³Ø§Ø³ÙŠØ©](#)
- [Ø§Ù,,Ù...Ø^Ø-Ù,,Ø·Ø§Ø^](#)
- [Ø§Ù,,Ù...ÙfÙ^Ù†Ø§Ø^ Ø§Ù,,Ù...Ø³Ø^Ø®Ø-Ù...Ø©](#)
- [Ø§Ù,,Ø^ÙfÙ^ÙŠÙ†](#)
- [Ø§Ù,,Ø±Ø³Ù... Ø§Ù,,Ø^Ø®Ø-ÙŠØ·ÙŠ Ù,,Ù,,Ø·Ø-ÙfØ© Ù^Ø^Ø-Ù◆Ù, ØØ±ÙfØ© Ù...Ø±Ù^Ø±](#)
- [Ø§Ù,,Ø·ÙŠØ§Ù†Ø§Ø^](#)
- [Ø§Ù,,Ø^ÙfÙ^ÙŠÙ†Ø§Ø^](#)
- FTD/FMC
- [Ù...ØØ±Ùf Ø®Ø-Ù...Ø§Ø^ ÙfØ-Ù◆ Ø§Ù,,Ù†Ù^ÙŠØ© \(ISE\)](#)
- [Ø§Ù,,Ø^ØÙ,Ù, Ù...Ù† Ø§Ù,,ØØØ©](#)
- [Ø§Ø³Ø^ÙfØ·Ø§Ù◆ Ø§Ù,,Ø£Ø®Ø·Ø§Ø; Ù^Ø¥ØµÙ,,Ø§ØÙ†Ø§](#)

Ø§Ù,,Ù...Ù,Ø-Ù...Ø©

ÙŠÙ^Ø¶Ø Ù†Ø°Ø§ Ø§Ù,,Ù...Ø³Ø^Ù†Ø- ÙfÙŠÙ◆ÙŠØ© Ø^ÙfÙ^ÙŠÙ† Ø§Ù,,Ø¥ØµØ¯Ø§Ø± 6.4.0 Ù...Ù† "Ø§Ù,,Ø-Ù◆Ø§Ø¹ Ø¹Ù† Ø^Ù†Ø-ÙŠØ- FirePOWER (FTD)" Ù,,Ø^Ù†ÙŠØ|Ø© Ù...Ø³Ø^Ø®Ø-Ù...ÙŠ VPN Ù...Ù,,Ø§Ø·Ù,, Ù...ØØ±Ùf Ø®Ø-Ù...Ø§Ø^ Ø§Ù,,Ù†Ù^ÙŠØ© (ISE).

Ø§Ù,,Ù...Ø^Ø·Ù,,Ø·Ø§Ø^ Ø§Ù,,Ø£Ø³Ø§Ø³ÙŠØ©

Ø§Ù,,Ù...Ø^Ø·Ù,,Ø·Ø§Ø^

Ø^Ù^Ø¶Š Cisco Ø·Ø£Ù† Ø^ÙfÙ^Ù† Ù,,Ø-ÙŠÙf Ù...Ø¹Ø±Ù◆Ø© Ø·Ø§Ù,,Ù...Ù^Ø§Ø¶ÙŠØ¹ Ø§Ù,,Ø^Ø§Ù,,ÙŠØ©:

- AnyConnect Remote Access VPN
- Ø^ÙfÙ^ÙŠÙ† VPN Ù,,Ù,,Ù^Ø¶^Ù,,Ø¹Ù† Ø·Ø¹Ø- Ø¹Ù,,Ù% FTD
- Ø®Ø-Ù...Ø§Ø^ Ù^Ø¶Ø¹ÙŠØ© Ù...ØØ±Ùf Ø®Ø-Ù...Ø§Ø^ Ø§Ù,,Ù†Ù^ÙŠØ©

Ø§Ù,,Ù...ÙfÙ^Ù†Ø§Ø^ Ø§Ù,,Ù...Ø³Ø^Ø®Ø-Ù...Ø©

Ø^Ø³Ø^Ù†Ø- Ø§Ù,,Ù...Ø¹Ù,,Ù^Ù...Ø§Ø^ Ø§Ù,,Ù^Ø§Ø±Ø-Ø© Ù◆ÙŠ Ù†Ø°Ø§ Ø§Ù,,Ù...Ø³Ø^Ù†Ø- Ø¥Ù,,Ù% Ø¥ØµØ¯Ø§Ø±Ø§Ø^ Ø§Ù,,Ø·Ø±Ø§Ù...Ø- Ø§Ù,,Ø^Ø§Ù,,ÙŠØ©:

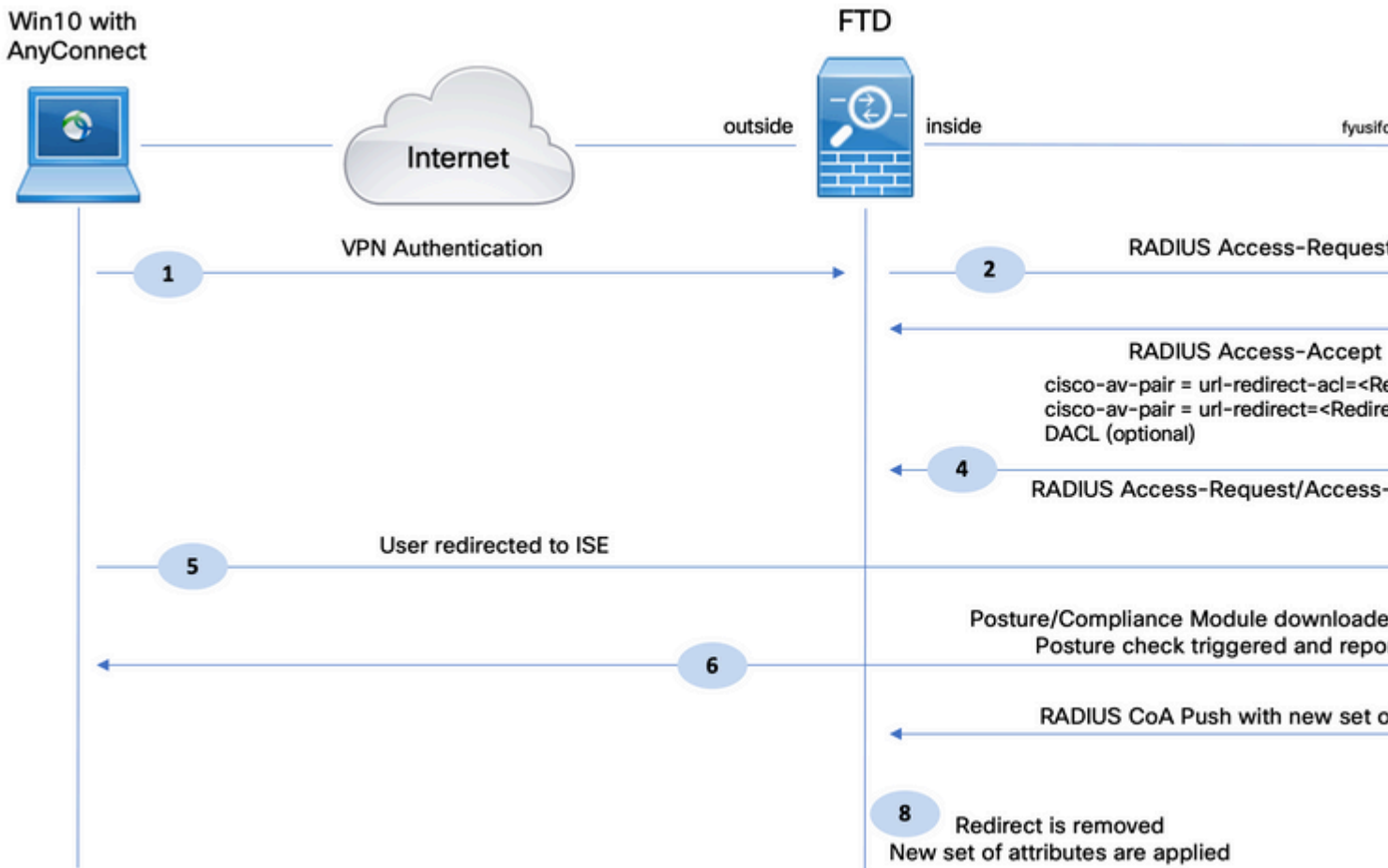
- Ø·Ø±Ù†Ø§Ù...Ø- Ø§Ù,,Ø-Ù◆Ø§Ø¹ Ø¹Ù† Ø^Ù†Ø-ÙŠØ- FirePOWER (FTD) Ù...Ù† CiscoØ£ Ø§Ù,,Ø¥ØµØ¯Ø§Ø± 6.4.0
- Ø·Ø±Ù†Ø§Ù...Ø- Cisco Firepower Management Console (FMC)Ø£ Ø§Ù,,Ø¥ØØ-Ø§Ø± 6.5.0
- Microsoft Windows 10 Ù...Ø¹ Cisco AnyConnect Secure Mobility ClientØ£ Ø§Ù,,Ø¥ØØ-Ø§Ø± 4.7
- Cisco Identity Services Engine (ISE)Ø£ Ø§Ù,,Ø¥ØØ-Ø§Ø± 2.6 Ù...Ø¹ Patch 3

Ø^Ù... Ø¥Ù†Ø·Ø§Ø; Ø§Ù,,Ù...Ø¹Ù,,Ù^Ù...Ø§Ø^ Ø§Ù,,Ù^Ø§Ø±Ø-Ø© Ù◆ÙŠ Ù†Ø°Ø§

1. Win10 with AnyConnect connects to FTD via Internet. FTD initiates RADIUS Access-Request to ISE. ISE responds with RADIUS Access-Accept containing attributes for URL redirection and DACL. FTD pushes RADIUS CoA to Win10. Win10 is redirected to ISE. FTD removes the redirect and applies new attributes.

Win10 with AnyConnect

Win10 with AnyConnect connects to FTD via Internet. FTD initiates RADIUS Access-Request to ISE. ISE responds with RADIUS Access-Accept containing attributes for URL redirection and DACL. FTD pushes RADIUS CoA to Win10. Win10 is redirected to ISE. FTD removes the redirect and applies new attributes.



- Win10 with AnyConnect connects to FTD via Internet. FTD initiates RADIUS Access-Request to ISE. ISE responds with RADIUS Access-Accept containing attributes for URL redirection and DACL. FTD pushes RADIUS CoA to Win10. Win10 is redirected to ISE. FTD removes the redirect and applies new attributes.
- Win10 with AnyConnect connects to FTD via Internet. FTD initiates RADIUS Access-Request to ISE. ISE responds with RADIUS Access-Accept containing attributes for URL redirection and DACL. FTD pushes RADIUS CoA to Win10. Win10 is redirected to ISE. FTD removes the redirect and applies new attributes.
- Win10 with AnyConnect connects to FTD via Internet. FTD initiates RADIUS Access-Request to ISE. ISE responds with RADIUS Access-Accept containing attributes for URL redirection and DACL. FTD pushes RADIUS CoA to Win10. Win10 is redirected to ISE. FTD removes the redirect and applies new attributes.

- cisco-av-pair = url-redirect-acl=fyusifovredirect** - URL redirection ACL (ACL) configuration on FTD.

Ù...ØÙ,,ÙŠØŠ Ø¹Ù,,Ù% FTDØCE Ù^ØŠÙ,,Ø°ÙŠ ÙŠÙ,Ø±Ø± ØØ±ÙfØ© Ù...Ø±Ù^Ø± ØŠÙ,,Ø°ÙŠØŠÙ†ØŠØª ØŠÙ,,ØªÙŠ ÙŠØªÙ... Ø¥Ø¹ØŠØ-Ø© ØªÙ^Ø-ÙŠÙ†Ù‡ØŠ.

- Cisco-av-pair = url-redirect=<https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp> - Ù‡Ø°Ø§ Ù‡Ù^ Ø¹Ù†Ù^Ø§Ù† URL Ø§Ù,,Ø°ÙŠ ÙŠØªÙ... Ø¥Ø¹ØŠØ-Ø© ØªÙ^Ø-ÙŠÙ† Ø§Ù,,Ù...Ø³ØªØ©Ø-Ù... Ø§Ù,,Ø°ÙŠØ- Ø¥Ù,,ÙŠÙ‡.
- **ACL = ALLOWED ALL IPv4 TRAFFIC** - Ù,Ø§Ø¡Ù...Ø© Ø§Ù,,ØªØÙfÙ... ÙØÙŠ ØŠÙ,,Ù^ØµÙ^Ù,, (ACL) ØŠÙ,,Ù,ØŠØ°Ù,,Ø© Ù,,Ù,,ØªÙ†Ø²ÙŠÙ,, Ù‡Ø°Ù‡ ØŠÙ,,Ø³Ù...Ø© Ø¥ØªØªØªÙŠØŠØ±ÙŠØ©. ÙØÙŠ Ù‡Ø°Ø§ ØŠÙ,,Ø³ÙŠÙ†ØŠØ±ÙŠÙ^ØCE ÙŠØªÙ... ØŠÙ,,Ø³Ù...ØŠØ Ø°Ø-Ù...ÙŠØ¹ ØØ±ÙfØŠØª Ù...Ø±Ù^Ø± ØŠÙ,,Ø°ÙŠØŠÙ†ØŠØª ÙØÙŠ Ù,ØŠØ¡Ù...Ø© ØŠÙ,,ØªØÙfÙ... ÙØÙŠ ØŠÙ,,Ù^ØµÙ^Ù,, ØŠÙ,,ØªØŠØµØ© Ø°ØŠÙ,,Ù...Ù†ÙØ° (ACL)

4. ÙØÙŠ ØØŠÙ,,Ø© Ø¥Ø±Ø³ØŠÙ,, Ù,ØŠØ¡Ù...Ø© ØŠÙ,,ØªØÙfÙ... ÙØÙŠ ØŠÙ,,Ù^ØµÙ^Ù,, Ù,,Ù,,Ø°Ù†ÙŠØ© ØŠÙ,,Ø£Ø³ØŠØ³ÙŠØ© (ACL)ØCE ÙŠØªÙ... ØªØ°ØŠØ-Ù,, Ø·Ù,,Ø°Ù^ØµÙ^Ù,, RADIUS/Ù,Ø°Ù^Ù,, ØŠÙ,,Ù^ØµÙ^Ù,, Ù...Ù† Ø£Ø-Ù,, ØªÙ†Ø²ÙŠÙ,, Ù...ØªÙ^Ù% Ù,ØŠØ¡Ù...Ø© ØŠÙ,,ØªØÙfÙ... ÙØÙŠ ØŠÙ,,Ù^ØµÙ^Ù,, Ù,,Ù,,Ø°Ù†ÙŠØ© ØŠÙ,,Ø£Ø³ØŠØ³ÙŠØ© (ACL)

5. Ø¹Ù†Ø- ØªØ·Ø§Ø-Ù, ØØ±ÙfØ© Ø§Ù,,Ù...Ø±Ù^Ø± Ù...Ù† Ù...Ø³ØªØ©Ø-Ù... Ø§Ù,,Ø°Ù^ØµÙ^Ù... Ø§Ù,,ØªØÙfÙ... Ø§Ù,,ØªØÙfÙ... Ø§Ù,,ØªØÙfÙ... ÙØÙŠ ØŠÙ,,Ù^ØµÙ^Ù,, (ACL) ØŠÙ,,Ù...ØØ-Ø-Ø© Ù...ØÙ,,ÙŠØŠØCE ØªØªÙ... Ø¥Ø¹ØŠØ-Ø© ØªÙ^Ø-ÙŠÙ†Ù‡ØŠ Ø¥Ù,,Ù% Ø°Ù^ØŠØ°Ø© Ø¥Ù...Ø-ØŠØ- Ø¹Ù...ÙŠÙ,, ISE. ØªÙ^ÙØ± ISE AnyConnect Posture Module Ù^Ù^ØØ-Ø© ØŠÙ,,ØªÙ^ØŠÙØÙ,,

6. Ø°Ø¹Ø- ØªØ«Ø°ÙŠØª Ø§Ù,,Ù^ØµÙ^Ù,, Ø¹Ù,,Ù% Ø-Ù‡Ø§Ø² Ø§Ù,,Ø¹Ù...ÙŠÙ,,ØCE ÙŠÙ,Ù^Ù... ØªÙ,,Ù,Ø§Ø¡ÙŠØ§ Ø°ØŠÙ,,Ø°Ø« Ø¹Ù† ISE Ø°Ø§Ø³ØªØªØ-Ø§Ù... Ø§Ù,,Ù...Ø³Ø§Ø°ÙŠØ±. Ø¹Ù†Ø- Ø§ÙfØªØ-Ø§ÙØ ISE Ø°Ù†Ø-ØŠØØCE ÙŠØªÙ... ØŠÙ,,ØªØÙ,Ù, Ù...Ù† Ù...ØªØ·Ù,,Ø°ØŠØª ØŠÙ,,Ù^Ø¶Ø¹ Ø¹Ù,,Ù% Ù†Ù,Ø·Ø© ØŠÙ,,Ù†Ù‡ØŠÙŠØ©. ÙØÙŠ Ù‡Ø°Ø§ ØŠÙ,,Ù...Ø«ØŠÙ,,ØCE ÙŠØªØÙ,Ù, ØŠÙ,,Ø¹Ù...ÙŠÙ,, Ù...Ù† Ù^Ø-Ù^Ø- Ø£ÙŠ Ø°Ø±Ù†ØŠÙ...Ø- Ù...Ø«Ø° Ù,,Ù...ÙfØŠÙØØ© ØŠÙ,,Ø°Ø±ØŠÙ...Ø- ØŠÙ,,Ø¶ØŠØ±Ø©. Ø«Ù... ÙŠØ±Ø³Ù,, ØªÙ,Ø±ÙŠØ± ØØŠÙ,,Ø© Ø¥Ù,,Ù% ISE.

7. Ø¹Ù†Ø-Ù...Ø§ ÙŠØ³ØªÙ,Ø·Ù,, ISE ØªÙ,Ø±ÙŠØ± Ø§Ù,,ØØ§Ù,,Ø© Ù...Ù† Ø§Ù,,Ù^ØµÙ^Ù,,ØCE ÙŠÙ,Ù^Ù... ISE Ø°ØªØ°ÙŠÙŠØ± ØØ§Ù,,Ø© Ø§Ù,,Ù^Ø¶Ø¹ Ù,,Ø-Ù,,Ø³Ø© Ø§Ù,,Ø¹Ù...Ù,, Ù‡Ø°Ù‡ Ù^ÙŠØ-Ù,,Ù, Ø-ÙØ¹ Ù†Ù^Ø¹ RADIUS CoA Ù...Ø¹ Ø³Ù...ØŠØª Ø-Ø-ÙŠØ-Ø©. Ù‡Ø°Ù‡ ØŠÙ,,Ù...Ø±Ø©ØCE ØªÙfÙ^Ù† ØØŠÙ,,Ø© ØŠÙ,,Ù^Ø¶Ø¹ Ù...Ø¹Ø±Ù^ÙØ© Ù^ÙŠØªÙ... ØŠÙ,,Ù^ØµÙ^Ù,, Ø¥Ù,,Ù% Ù,ØŠØ¹Ø-Ø© Ø£ØªØ±Ù%.

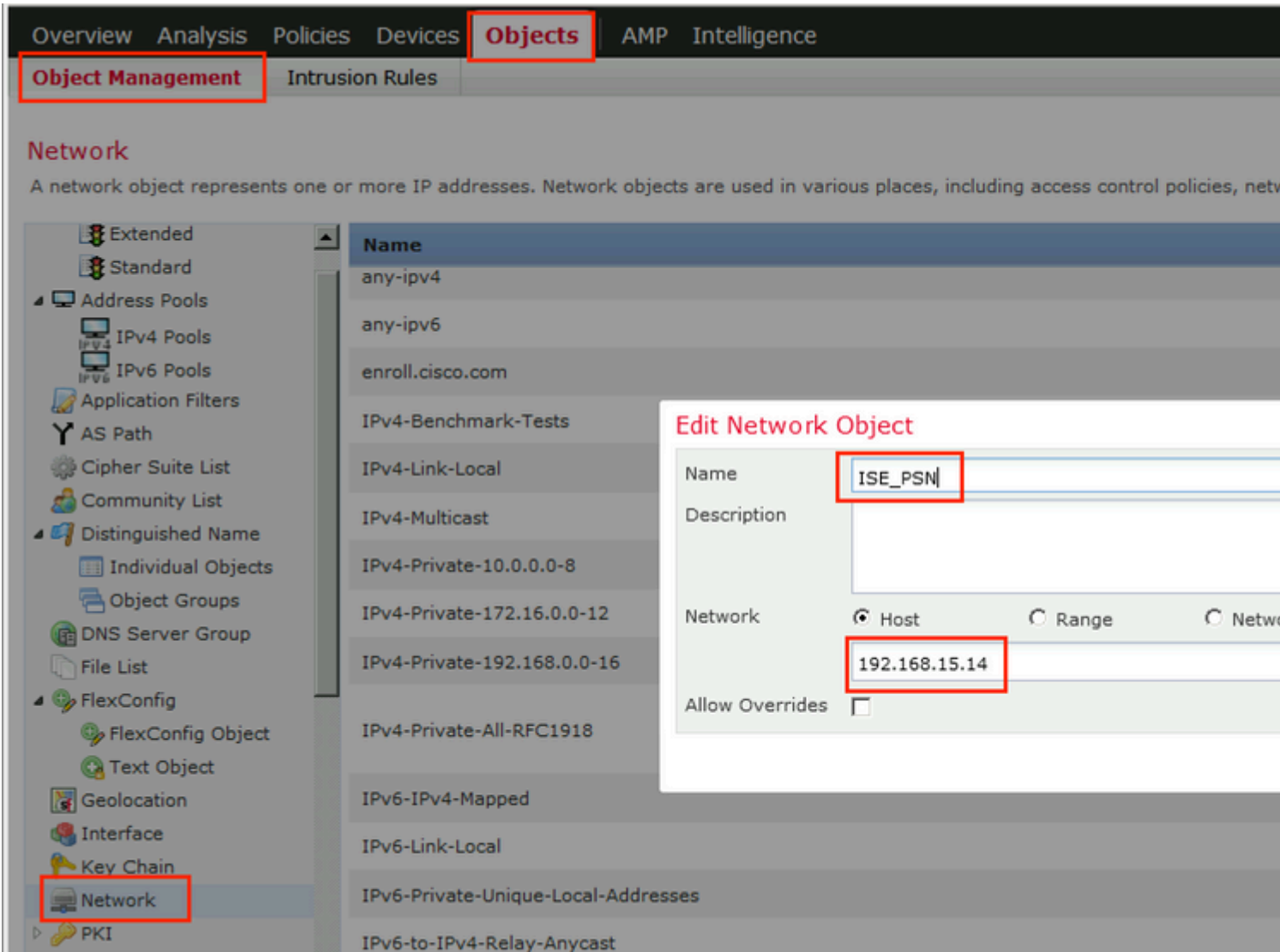
- Ø¥Ø°Ø§ ÙfØ§Ù† Ø§Ù,,Ù...Ø³ØªØ©Ø-Ù... Ù...ØªÙ^Ø§ÙØÙ,ØŠØCE ÙØÙŠÙŠØªÙ... Ø¥Ø±Ø³ØŠÙ,, ØŠØ³Ù... ACL ÙŠØ³Ù...Ø Ø°ØŠÙ,,Ù^ØµÙ^Ù,, ØŠÙ,,ÙfØŠÙ...Ù,,
- Ø¥Ø°Ø§ ÙfØ§Ù† Ø§Ù,,Ù...Ø³ØªØ©Ø-Ù... Ø°ÙŠØ± Ù...ØªÙ^Ø§ÙØÙ,ØCE ÙØÙŠÙŠØªÙ... Ø¥Ø±Ø³ØŠÙ,, ØŠØ³Ù... ACL ÙŠØ³Ù...Ø Ø°ØŠÙ,,Ù^ØµÙ^Ù,, ØŠÙ,,Ù...ØØ-Ù^Ø-

8. ÙŠØ²ÙŠÙ,, "Ø°Ø±Ù†Ø§Ù...Ø- Ø§Ù,,Ø¥Ø±Ø³Ø§Ù,, ÙØÙŠØ¡Ù, ØŠÙ,,Ø³Ø±Ø¹Ø© (FTD)" Ø¥Ø¹ØŠØ-Ø© ØŠÙ,,ØªÙ^Ø-ÙŠÙ‡. ÙŠØ±Ø³Ù,, FTD Ø·Ù,,Ø°ØŠÙ,,Ù^ØµÙ^Ù,, Ù...Ù† Ø£Ø-Ù,, ØªÙ†Ø²ÙŠÙ,, ACL Ù...Ù† ISE. ÙŠØªÙ... Ø¥Ø±ÙØÙ, Ù,ØŠØ¡Ù...Ø© ØŠÙ,,ØªØÙfÙ... ÙØÙŠ ØŠÙ,,Ù^ØµÙ^Ù,, (ACL) ØŠÙ,,Ù...ØØ-Ø-Ø© Ø°Ø-Ù,,Ø³Ø© Ø¹Ù...Ù,, ØŠÙ,,Ø°Ù^Ø-ÙfØ© ØŠÙ,,ØªØŠØµØ© ØŠÙ,,Ø,ØŠÙ‡Ø±ÙŠØ© (VPN).

Ø§Ù,,ØªÙfÙ^ÙŠÙ†Ø§Øª

FTD/FMC

Ø§Ù,,ØªØ·Ù´Ø© 1. Ù,Ù... Ø´Ø¥Ù†Ø´Ø§Øª; Ù...Ø-Ù...Ù´Ø¹Ø© ÙfØ§Øª!Ù†Ø§Øªª Ø§Ù,,Ø´Ø·ÙfØ© Ù,,ØªØ¹Ø§Øª-Ù... ISE Ù´Ø§Ù,,Ù...Ø¹Ø§Ù,,Ø-Ø© (Ø¥Ù† Ù´Ø-Ø-Øª). Ø§Ù†ØªÙ,,Ù,, Ø¥Ù,,Ù% ÙfØ§Øª!Ù†Ø§Øªª > Ø¥Ø´Ø§Øª±Ø© Ø§Ù,,ÙfØ§Øª!Ù† > Ø§Ù,,Ø´Ø·ÙfØ©.



Ø§Ù,,ØªØ·Ù´Ø© 2. Ø¥Ù†Ø´Ø§Øª; Ù,Ø§Øª!Ù...Ø© ØªØÙfÙ... Ù´ÙŠ Ø§Ù,,Ù´ØµÙ^Ù,, (ACL) Ù,,Ø¥Ø¹Ø§Øª-Ø© Ø§Ù,,ØªÙ´ØªÙ¸. Ø§Ù†ØªÙ,,Ù,, Ø¥Ù,,Ù% ÙfØ§Øª!Ù†Ø§Øªª > Ø¥Ø´Ø§Øª±Ø© Ø§Ù,,ÙfØ§Øª!Ù† > Ù,Ø§Øª!Ù...Ø© Ø§Ù,,Ù´ØµÙ^Ù,, > Ù...Ù´Ø³Ø¹. Ø§Ù†Ù,,Ø± Ù´Ù^Ù,, Ø¥Ø¶Ø§Ù´Ø© Ù,Ø§Øª!Ù...Ø© Ø§Ù,,Ù´ØµÙ^Ù,, Ø§Ù,,Ù...Ù´Ø³Ø¹Ø© Ù´ØªÙ,,Ø-ÙŠÙ... Ø§Ø³Ù... Ù,Ø§Øª!Ù...Ø© Ø§Ù,,ØªØÙfÙ... Ù´ÙŠ Ø§Ù,,Ù´ØµÙ^Ù,, (ACL) Ù,,Ø¥Ø¹Ø§Øª-Ø© Ø§Ù,,ØªÙ´ØªÙ¸. ÙŠØ-Ø´ Ø£Ù† ÙŠÙfÙ^Ù† Ù±Ø°Ø§ Ø§Ù,,Ø§Ø³Ù... Ù±Ù^ Ù†Ù´Ø³Ù¸ Ø§Ù,,Ù...Ù´Ø-Ù^Ø´ Ù´ÙŠ Ù†ØªÙŠØ-Ø© ØªØªØ¹ÙŠÙ,, ISE.

The screenshot shows the Cisco FMC interface with the 'Objects' tab selected. The left sidebar contains a tree view with 'Access List' expanded to show 'Extended'. The main content area is titled 'New Extended Access List Object' and contains a form with the following fields:

- Name:** fyusifovredirect
- Entries (0):** A table with columns: Sequence, Action, Source, Source Port, Destination. The table is empty, displaying 'No records to display'.
- Allow Overrides:**

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Add Extended Access List Entry

Action: ✖ Block ▼

Logging: Default ▼

Log Level: Informational ▼

Log Interval: Sec.

Network | Port

Available Networks ↻ +

- any
- any-ipv4
- any-ipv6
- enroll.cisco.com
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Source Networks (1)

any-ipv4 ✕

Destination

ISE_... ✕

Edit Extended Access List Object

Name:

Entries (4)

Sequence	Action	Source	Source Port	Destination	Desti
1	✖ Block	any	Any	Any	DN
2	✖ Block	any-ipv4	Any	ISE_PSN	Any
3	✖ Block	any-ipv4	Any	RemediationServers	Any
4	✔ Allow	any-ipv4	Any	any-ipv4	Any

Allow Overrides

0x00000000 4. 0x00000000 0x00000000 ISE PSN. 0x00000000, 0x00000000
 0x00000000 > 0x00000000 0x00000000 0x00000000 > 0x00000000... 0x00000000... RADIUS.
 0x00000000, 0x00000000 0x00000000 0x00000000... 0x00000000... RADIUS 0x00000000...
 0x00000000, 0x00000000 0x00000000... 0x00000000... 0x00000000... 0x00000000... 0x00000000...

08085Ù+080ª 08Ù,,080®0ªÙš080± Ù^08Ù+Ù,0± Ù◆Ù^Ù, 0EÙšÙ,Ù^Ù+0© 0²0§0:0.

Edit RADIUS Server Group

Name:*

ISE

Description:

Group Accounting Mode:

Single

Retry Interval:*

10

(1-10)

Realms:

Enable authorize only

Enable interim account update

Interval:*

24

(1-12)

Enable dynamic authorization

Port:*

1700

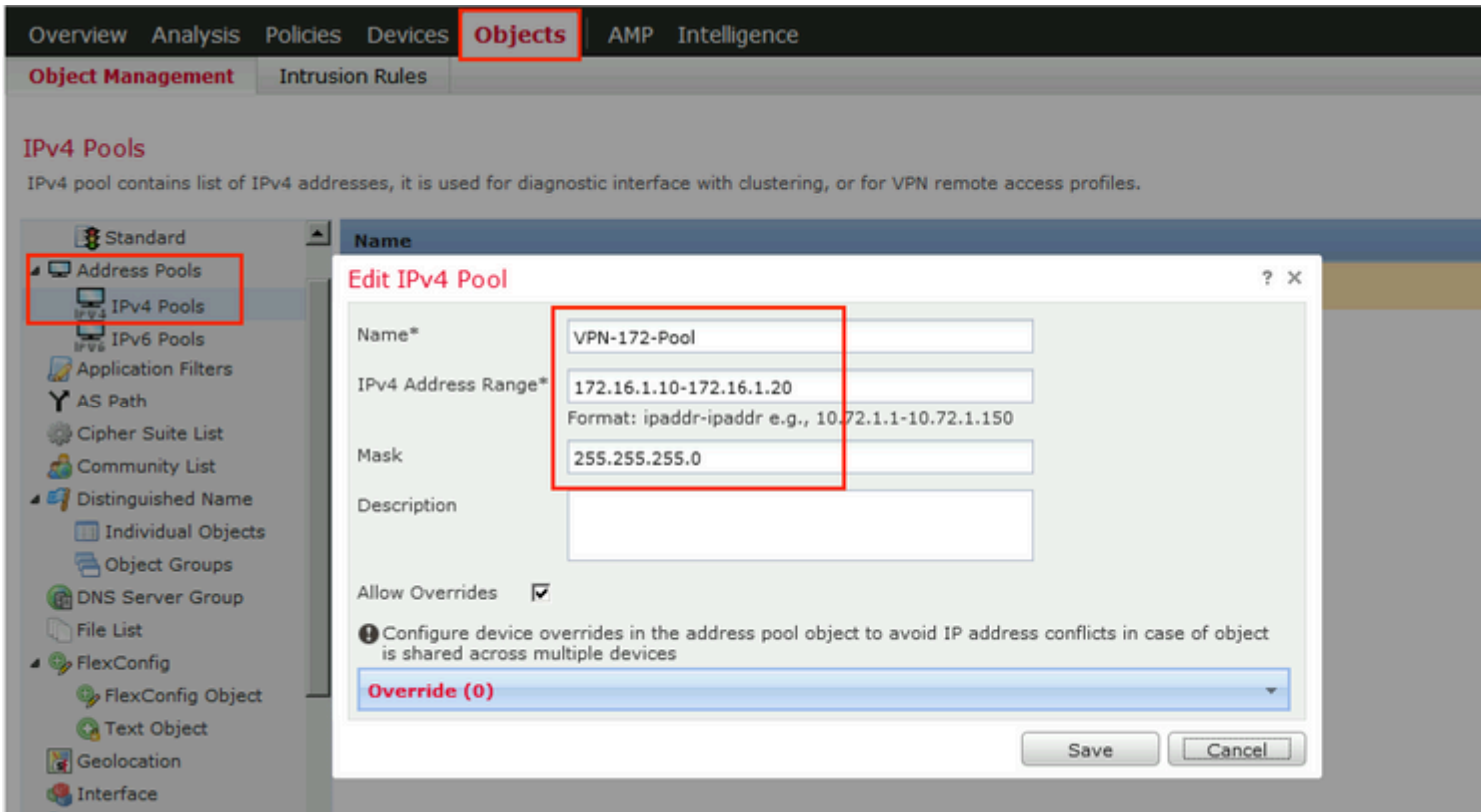
(1024)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname

No records to display

0§Ù,,000·Ù^0© 5.



0\$Ù,,0@0·Ù^0© 7. 0¥Ù†0'0\$0; 00²Ù...0© AnyConnect. 0\$Ù†0ªÙ,Ù,, 0¥Ù,,Ù% Ùf0\$0:Ù†0\$0ª >
 0¥0-0\$0±0© 0\$Ù,,Ùf0\$0:Ù† > VPN > Ù...Ù,,Ù ♦ AnyConnect. 0\$Ù†Ù,0± Ù ♦ Ù^Ù,
 0¥0¶0\$Ù ♦ 0© Ù...Ù,, Ù ♦ AnyConnect0Æ Ù^0£0-0@Ù,, 0\$0³Ù... 0\$Ù,,00²Ù...0©0Æ
 Ù^Ù,Ù... 0'0ªÙ†0²ÙšÙ,, 0\$Ù,,00²Ù...0© Ù...Ù† 0ªÙ†0²ÙšÙ,, 0'0±0\$Ù...0¬ Cisco Software
 Ù^00-0- Ù†Ù^0¹ Ù...Ù,,Ù ♦ 0µ^0±0© 0¹Ù...ÙšÙ,, AnyConnect.

Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing activities occur in your Private Key Infrastructure (PKI).

- Access List
- Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- DNS Server Group
- File List
- FlexConfig
- Geolocation
- Interface
- Key Chain
- Network
- PKI**
 - Cert Enrollment**
 - External Cert Groups
 - External Certs
 - Internal CA Groups
 - Internal CAs
 - Internal Cert Groups
 - Internal Certs
 - Trusted CA Groups
 - Trusted CAs
- Policy List
- Port

Add Cert Enrollment

Name*

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

⚠ Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides

Save

Cancel

Add Cert Enrollment

Name*

vpn-cert

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Use Device Hostname as FQDN

Include Device's IP Address:

10.48.26.99

Common Name (CN):

vpn-cert.example.com

Organization Unit (OU):

Organization (O):

example

Locality (L):

State (ST):

Krakow

Country Code (C):

PL

Email (E):

Include Device's Serial Number

Allow Overrides

0\$Ù,,0@0-Ù^0© 9. 0^0^0^ÙŠÙ,, Ù...0^0\$Ù,,0^ VPN Ù,,Ù,,Ù^0µ^Ù,, 0^Ù† 0^0^0^ . 0\$Ù†0^Ù,, Ù,, 0\$Ù,,Ù% 0\$Ù,,0£0-Ù‡0^0© > VPN > 0\$Ù,,Ù^0µ^Ù,, 0^Ù† 0^0^0^ Ù^0\$Ù†Ù,,0± Ù^Ù,, 0\$0¶0\$Ù^0©.

Overview Analysis Policies **Devices** Objects AMP Intelligence
 Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Name	Status	Last Modified
No configuration available Add a new configuration		

Ø§Ù,,Ø®Ø·Ù`Ø© 10. Ù, Ù... Ø·ØªÙ`Ù`Ø±ÙŠØ± Ø§Ù,,Ø§Ø³Ù...Ø¸ Ù`Ù`ØØµ SSL Ù¸Ø·Ø±Ù`ØªÙ`Ù¸Ù`Ù,, VPNØ¸ Ù`Ø§Ø®ØªªØ± FTD Ø§Ù,,Ø°ÙŠ ÙŠØªÙ... Ø¥Ø³ªªØ®Ø¯Ø§Ù...Ù‡ Ù¸Ù...Ø±Ù¸Ø² VPN Ù`Ø§Ù¸Ù¸Ù,Ø± Ø¹Ù,,Ù% Ø§Ù,,ØªØ§Ù,,ÙŠ.

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name: *

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: Available Devices Selected Devices

Search

192.168.15.11

192.168.15.11

Add

Before You Start

Before you start, ensure that the following configuration elements are in place to complete Remote Access VPN configuration:

Authentication Server
Configure [Realm](#) or [Group](#) to authenticate VPN clients.

AnyConnect Client Package
Make sure you have the AnyConnect Client package for VPN Client installed on the targeted devices. You must have the relevant version of the package to download it during the configuration process.

Device Interface
Interfaces should be available on targeted [devices](#) so that they can be used as a security zone. You must assign the interface to a group to enable VPN access.

Ø§Ù,,Ø®Ø·Ù`Ø© 11. ØªÙ`Ù`Ø±ÙŠØ± Ø§Ø³Ù... Ù...Ù,,Ù`ØªØ¹Ø±ÙŠÙ`Ø± Ø§Ù,,Ø§ØªØµØ§Ù,,Ø¸ Ù`ØªØØ-ÙŠØ- Ø®Ù`Ø§ØØ-Ù... Ø§Ù,,Ù...Ø¸Ø§ØØ-Ù,,Ø©/Ø§Ù,,Ù...Ø¸Ø§Ø³Ø·Ø©Ø¸ Ù`ØªØØ-ÙŠØ- ØªØ-Ù...Ø¹ Ø§Ù,,Ø¹Ù¸Ø§Ù¸Ù`ÙŠÙ¸ Ø§Ù,,Ø°ÙŠ ØªÙ... ØªÙ¸Ù`Ù¸Ù¸Ù¸Ù¸ Ù...Ø³Ø·Ù,,Ø§Ø¸ Ø«Ù... Ø§Ù¸Ù¸Ù,Ø± Ø¹Ù,,Ù% Ø§Ù,,ØªØ§Ù,,ÙŠ.

Ù...Ù,,Ø§ØØØ,Ø©: Ù,,Ø§ ØªØØ-Ø- Ø®Ø§ØØ-Ù... Ø§Ù,,ØªØ®Ù`Ù¸Ù¸,, Ù`Ù¸Ù`Ù` ÙŠØ·Ø°Ù,, Ø·Ù,,Ø·Ù¸Ù¸Ù¸ Ù,,Ù,,Ù`Ø¸Ù`Ù,, Ù,,Ù...Ø³ªªØ®Ø¯Ù... Ù`Ø§ØØØ- (Ù...Ø±Ø© Ù`Ø§ØØØ-Ø© Ø·Ø§Ø³ªªØ®Ø¯Ø§Ù¸... Ù¸Ù,,Ù...Ø© Ù...Ø±Ù`Ø± Ø§Ù,,Ù...Ø³ªªØ®Ø¯Ù... Ù`Ù...Ø±Ø© Ø«Ø§Ù¸Ù¸Ù¸Ø© Ø·Ø§Ø³ªªØ®Ø¯Ø§Ù¸... Ù¸Ù,,Ù...Ø© Ø§Ù,,Ù...Ø±Ù`Ø± cisco).

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

EmployeeVPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

AAA Only

Authentication Server:*

ISE

(Realm or RADIUS)

Authorization Server:

Use same authentication server

(RADIUS)

Accounting Server:

ISE

(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address

VPN-172-Pool

IPv6 Address

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*

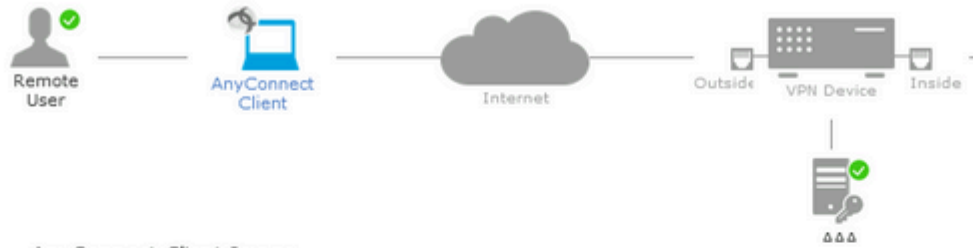
DfltGrpPolicy

[Edit Group Policy](#)

Ø§Ù,,Ø@Ø·Ù^Ø© 12. ØØ^Ø^ ØØ²Ù...Ø© AnyConnect Ø§Ù,,ØªÙŠ ØªÙ... ØªÙfÙ^ÙŠÙ†Ù‡Ø§
Ù...Ø³Ø^Ù,Ø§ Ù^Ø§Ù†Ù,Ø± Ù^Ù^Ù, Ø§Ù,,ØªØ§Ù,,ÙŠ.

Remote Access VPN Policy Wizard

- 1 Policy Assignment
- 2 Connection Profile
- 3 AnyConnect
- 4 Access & Certificate
- 5 Summary



AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#)

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AC47	anyconnect-win-4.7.01076-webdeploy-k9....	Windows

Ø§Ù,,Ø@Ø·Ù^Ø© 13. Ø§Ù†ØªÙ,ÙŠØª Ù,Ø§Ø±Ù† Ù...Ù† Ø£ÙŠ VPN ØØ±ÙfØ© Ù...Ø±Ù^Ø± ÙŠÙfÙ^Ù† Ù...ØªÙ^Ù,Ø¹ØÆ Ø¹ÙŠÙ†Øª Ø¹Ù†Ø§Ø-Ø© ØªØ³Ø-ÙŠÙ,, Ø£Ù† ÙfØ§Ù† Ø¹fÙ,,Øª Ø³Ø§Ø·Ù,Ø§ Ù^Ø·Ù,Ø·Ù,Ø© Ø¹Ø¹Ø- Ø°Ù,,Ùf.

Remote Access VPN Policy Wizard

- 1 Policy Assignment
- 2 Connection Profile
- 3 AnyConnect
- 4 Access & Certificate
- 5 Summary

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* 
 Enable DTLS on member interfaces

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* 
 Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.










0x5,0@0.Û·0© 14. 0°0Û,Û, Û...Û† 0µ◆00© 0SÛ,,Û...Û,,0@0µ Û^0SÛ†Û,0± Û◆Û^Û,
0YÛ†Û‡0S0;

Remote Access VPN Policy Wizard

- 1 Policy Assignment
- 2 Connection Profile
- 3 AnyConnect
- 4 Access & Certificate
- 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

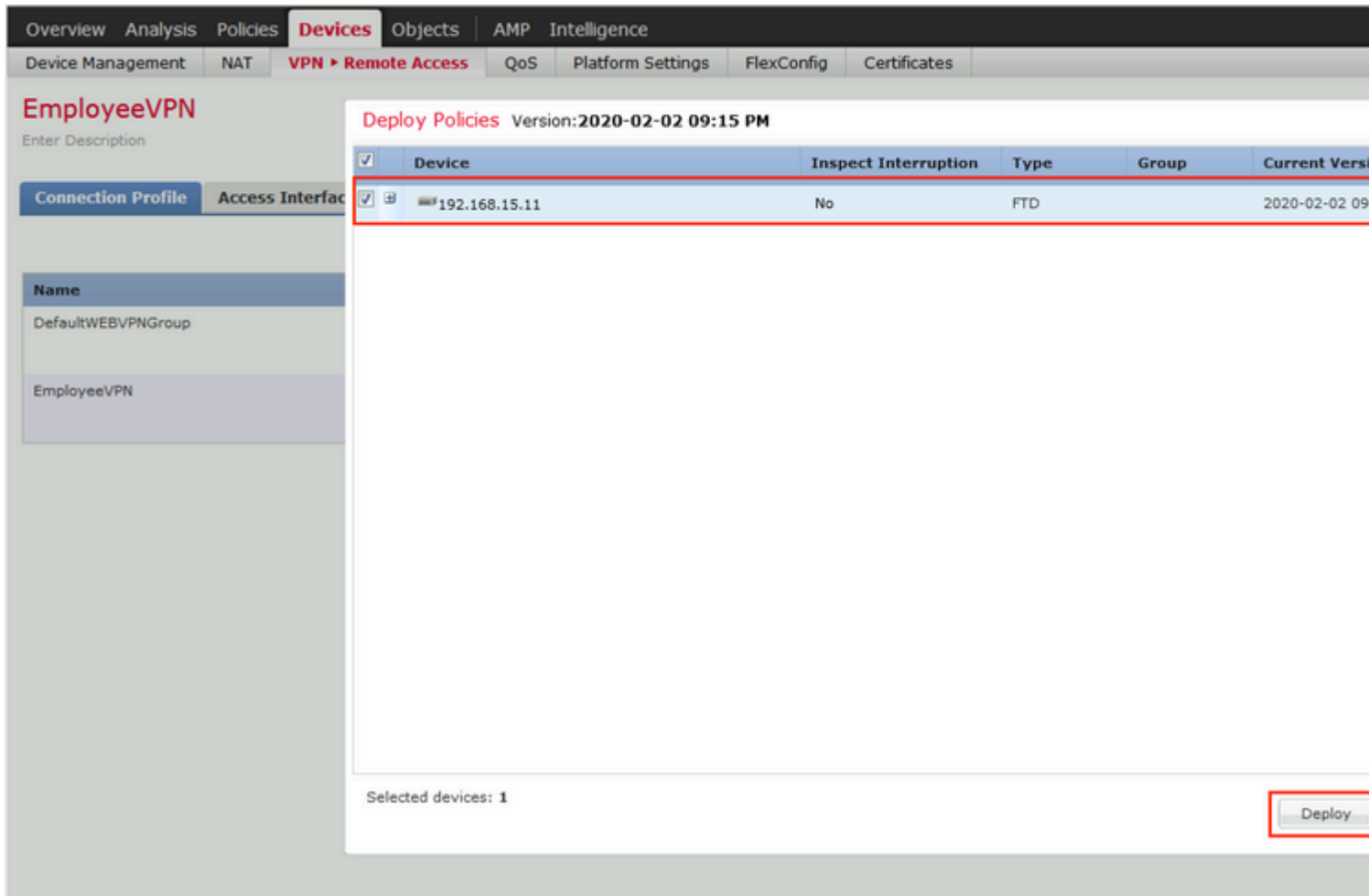
Name: EmployeeVPN
Device Targets:  192.168.15.11
Connection Profile: EmployeeVPN
Connection Alias: EmployeeVPN
AAA:
Authentication Method: AAA Only
Authentication Server:  ISE
Authorization Server:  ISE
Accounting Server:  ISE
Address Assignment:
Address from AAA: -
DHCP Servers: -
Address Pools (IPv4):  IPv4 VPN-172-Pool
Address Pools (IPv6): -
Group Policy:  DfltGrpPolicy
AnyConnect Images:  AC47
Interface Objects:  ZONE-OUTSIDE
Device Certificates:  vpn-cert

Additional Configuration Required

After the wizard completes, configuration needs to be completed on all device targets.

- 1 Access Control Policy Update
An [Access Control](#) rule must allow VPN traffic on all targeted devices.
- 1 NAT Exemption
If NAT is enabled on the target devices, you must define a [NAT Policy](#) for VPN traffic.
- 1 DNS Configuration
To resolve hostname special characters on target devices, configure [FlexConfig Policy](#) on the target devices.
- 1 Port Configuration
SSL will be enabled on port 443. Please ensure that these ports are open on target devices in [NAT Policy](#) or other server configuration when deploying the configuration.
- 1 Network Interface Configuration
Make sure to add interface configuration on target devices to SecurityZone of OUTSIDE.

Step 15. Configure the FTD device to allow VPN access.



Step 16. Configure the ISE to allow VPN access.

Step 1. Configure the ISE to allow VPN access.

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

Proxy Port HH MM SS

Automatically check for updates starting from initial delay every

▼ Update Information

Last successful update on	2020/02/02 20:44:27 ⓘ
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:
Cisco conditions version	257951.0.0.0
Cisco AV/AS support chart version for windows	227.0.0.0
Cisco AV/AS support chart version for Mac OSX	148.0.0.0
Cisco supported OS version	49.0.0.0

Ø§Ù,,Ø@Ø·Ù·Ø© 2. Ù·ØØ-Ø© Ø§Ù,,ØªÙ·Ø§Ù·ØÙ, Ù...Ø¹ Ø§Ù,,ØªØÙ...ÙŠÙ,, Ø§Ù+ØªÙ,Ù,, Ø¥Ù,,Ù% Ø§Ù,,Ø³ÙŠØ§Ø³Ø© > Ø¹Ù†Ø§ØØ± Ø§Ù,,Ø³ÙŠØ§Ø³Ø© > Ø§Ù,,Ù†ØªØ§Ø!Ø- > Ø¥Ù...Ø-Ø§Ø- Ø§Ù,,Ø¹Ù...ÙŠÙ,, > Ø§Ù,,Ù...Ù·Ø§Ø±Ø·. Ø§Ù†Ù,Ø± Ù·ØÙ^Ù, Ø¥Ø¶Ø§Ù·Ø© Ù·ØØ-Ø- Ù...Ù·Ø§Ø±Ø- Ø§Ù,,Ù·Ù†ÙŠÙ,, Ù...Ù† Ù...Ù·Ù,Ø¹ Cisco

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance M
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance M
<input type="checkbox"/>	CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With C
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows V
<input type="checkbox"/>	ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.1
<input type="checkbox"/>	MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.1
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for M

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource" option, to import into ISE

Ø§Ù,,Ø@Ø·Ù^Ø© 3. Ù,Ù... Ø·ØªÙ†Ø²ÙŠÙ,, AnyConnect Ù...Ù† ØªÙ†Ø²ÙŠÙ,, Ø·Ø±Ø§Ù...Ø¬
[Cisco](#)Øœ Ø«Ù... Ù,Ù... Ø·ØªØÙ...ÙŠÙ,,Ù‡ Ø¥Ù,,Ù% ISE. Ø§Ù†ØªÙ,,Ù,, Ø¥Ù,,Ù%
Ø§Ù,,Ø³ÙŠØ§Ø³Ø© > Ø¹Ù†Ø§Ø± Ø§Ù,,Ø³ÙŠØ§Ø³Ø© > Ø§Ù,,Ù†ØªØ§Ø¬Ø¬ > Ø¥Ù...Ø¬Ø§Ø¬
Ø§Ù,,Ø¹Ù...ÙŠÙ,, > Ø§Ù,,Ù...Ù^Ø§Ø±Ø¬.

Ø§Ù†Ù,,Ø± Ù♦Ù^Ù, Ø¥Ø¶Ø§Ù♦Ø© Ù¬ØØØ Ù...Ù^Ø§Ø±Ø¬ Ø§Ù,,Ù^ÙfÙŠÙ,, Ù...Ù†
Ø§Ù,,Ù,Ø±Ø¶Ø§Ù,,Ù...ØÙ,,ÙŠ. Ø£Ø@ØªØ± Ø²Ù... Cisco Ø§Ù,,Ù...Ù,Ø¬Ù...Ø© Ø¶Ù...Ù†
Ø§Ù,,Ù♦Ø!Ø©Øœ Ù¬ØØØ Ø²Ù...Ø© AnyConnect Ù...Ù† Ø§Ù,,Ù,Ø±Ø¶Ø§Ù,,Ù...ØÙ,,ÙŠ
Ù^Ø§Ù†Ù,,Ø± Ù♦Ù^Ù, Ø¥Ø±Ø³Ø§Ù,,.

Agent Resources From Local Disk

Category

Cisco Provided Packages

Browse...

anyconnect-win-4.7.01076-webdeploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secu...

Submit Cancel

AnyConnect Posture. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0.

AnyConnect Posture. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0.

AnyConnect Posture. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0. AnyConnect Desktop Windows 4.7.1076.0.

* Name:

AC Posture Profile

Description

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if failure
Discovery host	<input type="text" value="1.2.3.4"/>		The server that the agent should connect to
* Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated server names that the agent can connect to. E.g. *.ci
Call Home List	<input type="text"/>	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that the agent will try to connect to if the PSN is unreachable for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continue to connect to targets and previously connected targets until max time limit is reached

0x00000000 5. 0x00000000, 0x00000000, 0x00000000 0x00000000 > 0x00000000 0x00000000
 > 0x00000000, 0x00000000:0x00000000 > 0x00000000...0x00000000 0x00000000, 0x00000000...0x00000000,
 > 0x00000000, 0x00000000...0x00000000 0x00000000, 0x00000000...0x00000000
 0x00000000 AnyConnect. 0x00000000, 0x00000000 0x00000000, 0x00000000 0x00000000
 AnyConnect. 0x00000000...0x00000000 AnyConnect 0x00000000 0x00000000... 0x00000000...
 0x00000000, 0x00000000...0x00000000 0x00000000 0x00000000, 0x00000000...0x00000000
 0x00000000 0x00000000 0x00000000 0x00000000, 0x00000000...0x00000000 0x00000000
 0x00000000 0x00000000...0x00000000, 0x00000000...0x00000000 0x00000000...

* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC CF 47

Description:

Description Value

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC_Posture_Profile

VPN

Network Access Manager

Web Security

AMP Enabler

Network Visibility

Umbrella Roaming Security

Customer Feedback

0\$Ù,,0@0·Ù·0© 6. 0\$Ù†0ªÙ,Ù,, 0¥Ù,,Ù% Ù†Ù‡0¬ > 0¥Ù...0-0\$0- 0\$Ù,,0¹Ù...ÙŠÙ,,
Ù¬0¥Ù†0-0\$0; 0³ÙŠ0\$0³0© 0¥Ù...0-0\$0- 0\$Ù,,0¹Ù...ÙŠÙ,, 0\$Ù†Ù,0± Ù◆Ù^Ù,
0ª00±ÙŠ0± 0«Ù... 00-0- 0¥0-0±0\$0¬ 0\$Ù,,Ù,0\$0¹0-0© 0£0¹Ù,,0\$Ù‡0œ Ù,Ù...
0·0ªÙ^Ù

◆ ÛŠ± ØŠÛ,,ØŠ³Û...Øœ ÛˆØˆˆ Û†Ø,ØŠÛ... ØŠÛ,,Ø³ØˆÛŠÛ,,Øœ ÛˆØŠØ®Ø³±
 Ø³ÛˆÛŠÛ† AnyConnect ØŠÛ,,Ø³Û Ø³Û... ØœÛ†ØˆØŠØ± Û◆ ÛŠ ØŠÛ,,Ø®Ø·ÛˆØœ
 ØŠÛ,,Ø³ØŠØˆÛ,Øœ.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
✓ AC_47_Win	If Any	and Windows All	and Condition(s)	then AC_CF_47
✓ IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
✓ Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
✓ Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
✓ MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.7.00135 And MacOSXSPWizard 2.1.0.42 And Cisco-ISE-NSP
✓ Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

ØŠÛ,,Ø®Ø·ÛˆØœ 7. Û,Û... ØˆØœÛ†ØˆØŠØ; ØØŠÛ,,Øœ Ø³Ø³ ØŠÛ,,Ø³ÛŠØŠØ³Øœ > Ø³Û†ØŠØ±
 ØŠÛ,,Ø³ÛŠØŠØ³Øœ > ØŠÛ,,Øˆ±ÛˆØˆ > ØŠÛ,,ÛˆØ¶Ø³ > ØØŠÛ,,Øœ ØŠÛ,,ØÛ...ØŠÛŠØœ Û...Û†
 ØŠÛ,,Øˆ±ØŠÛ...Øˆ ØŠÛ,,Ø¶ØŠØ±Øœ. Û◆ ÛŠ Û†ØˆØŠ ØŠÛ,,Û...ØœØŠÛ,,Øœ ÛŠØ³Û...
 ØœØ³Ø³Ø®ØˆØŠÛ... "ANY_am_win_inst" ØŠÛ,,Û...ØØˆ Û...Ø³ØˆÛ,ØŠ.

The screenshot displays the Cisco ISE web interface. At the top, the navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. Below this, a secondary menu shows 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. Under 'Policy Elements', 'Conditions' is selected, leading to a list of condition types: Library Conditions, Smart Conditions, Time and Date, Profiling, Posture, Anti-Malware Condition, Anti-Spyware Condition, Anti-Virus Condition, Application Condition, Compound Condition, Disk Encryption Condition, File Condition, and Firewall Condition. The 'Posture' category is expanded, and 'Anti-Malware Condition' is highlighted. The main content area is titled 'Anti-Malware Conditions' and features a table with columns for 'Name' and 'Description'. The table lists four conditions: 'ANY_am_win_inst', 'ANY_am_win_def', 'ANY_am_mac_inst', and 'ANY_am_mac_def'. The 'ANY_am_win_inst' entry is highlighted with a red box. Above the table are icons for 'Edit', 'Add', 'Duplicate', and 'Delete'.

8. `ANY_AM_INSTALLATION_WIN` - Any AM installation check on Windows

9. `ANY_AM_INSTALLATION_MAC` - Any AM installation check on Mac OS

Cisco Identity Services Engine			
Home	Context Visibility	Operations	Policy
Administration	Work Centers		
Policy Sets	Profiling	Posture	Client Provisioning
Dictionary	Conditions	Results	Policy Elements
Authentication	Authorization	Profiling	Posture
Remediation Actions	Requirements	Client Provisioning	

Name	Operating Systems	Compliance Module	Posture
Any_AV_Definition_Mac AnyAVDefRemediationMac	for Mac OSX	using 3.x or earlier	using AnyConnect
Any_AS_Installation_Mac Message Text Only	for Mac OSX	using 3.x or earlier	using AnyConnect
Any_AS_Definition_Mac AnyASDefRemediationMac	for Mac OSX	using 3.x or earlier	using AnyConnect
Any_AM_Installation_Win Message Text Only	for Windows All	using 4.x or later	using AnyConnect
Any_AM_Definition_Win AnyAMDefRemediationWin	for Windows All	using 4.x or later	using AnyConnect
Any_AM_Installation_Mac Message Text Only	for Mac OSX	using 4.x or later	using AnyConnect
Any_AM_Definition_Mac AnyAMDefRemediationM	for Mac OSX	using 4.x or later	using AnyConnect

Ø§Ù,,Ø®Ø·Ù´Ø© 10. Ù, Ù... Ø´Ø¥Ù´Ø´Ø§Ø; Ø³ÙØ§Ø³Ø§Øª Ø§Ù,,Ù´Ø¶Ø¹ ØªØªª Ø³ÙØ§Ø³Ø§Øª > Posture (Ù´Ø¶Ø¹ÙØ©). ÙØªÙ... Ø¥ØªªØ®Ø´Ø§Ù... Ù´ÙØ¬ Ø§Ù,,Ù´Ø¶Ø¹ Ø§Ù,,Ø§ÙØª±Ø§Ø¶ÙÙ Ù,,Ø£Ù ÙØªØµ AntiWare Ù,,Ù´Ø,Ø§Ù... ØªØ´Ø°ÙÙ,, Windows.

Cisco Identity Services Engine								
Home	Context Visibility	Operations	Policy	Administration	Work Centers			
Policy Sets	Profiling	Posture	Client Provisioning	Policy Elements				
Posture Policy								
Define the Posture Policy by configuring rules based on operating system and/or other conditions.								
Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	
⊖	Policy Options	Default_AntiMalware_Policy_Mac	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then
⊖	Policy Options	Default_AntiMalware_Policy_Mac_temporal	Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then
⊕	Policy Options	Default_AntiMalware_Policy_Win	Any	and Windows All	and 4.x or later	and AnyConnect	and	then
⊖	Policy Options	Default_AntiMalware_Policy_Win_temporal	Any	and Windows All	and 4.x or later	and Temporal Agent	and	then
⊖	Policy Options	Default_AppVis_Policy_Mac	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then

Ø§Ù,,Ø®Ø·Ù´Ø© 11. Ø§Ù´ØªÙ, Ù,, Ø¥Ù,,Ù% Ø§Ù,,Ø³ÙØ§Ø³Ø© > Ø¹Ù´Ø§Øª± Ø§Ù,,Ø³ÙØ§Ø³Ø© > Ø§Ù,,Ù´ØªØ§Ø:Ø¬ > Ø§Ù,,ØªÙÙØ¶ > Ù, Ù´Ø§Ø¶; Ù... Ø§Ù,,ØªØ·ÙÙ... ÙÙ Ø§Ù,,Ù´ØµÙ´Ù,, (ACL) Ø§Ù,,Ù,Ø§Ø´ Ù,,Ø© Ù,,Ù,,ØªÙ´Ø²ÙÙ,, Ù´Ø¥Ù´Ø´Ø§Ø; Ù, Ù´Ø§Ø:Ù... Ø§Ù,,ØªØ·ÙÙ... ÙÙ Ø§Ù,,Ù´ØµÙ´Ù,, (DACL) Ù,,Ù...Ø®ØªÙ,,Ù Ø§Ù,,Ø§Øª Ø§Ù,,Ù´Ø¶Ø¹.

ÙÙ ÙØªØ§ Ø§Ù,,Ù...Ø«Ø§Ù,,:

- Posture Unknown DACL - ÙØ³Ù...Ø´Øª±ÙØ© Ø§Ù,,Ù...Ø±Ù´Ø± Ø¥Ù,,Ù% Øª±ÙØ©

Ù...Ø±Ù^Ø± DNS Ù^ PSN Ù^ HTTP Ù^ HTTPS.

- Posture NonCompliant DACL - ÙŠØ±Ù^Ø± Ø§Ù,,Ù^ØµÙ^Ù,, Ø¥Ù,,Ù%Ø§Ù,,Ø'Ø' Ù^Ø§Øª Ø§Ù,,Ù^Ø±Ø¹ÙŠØ© Ø§Ù,,Ø®Ø§ØµØ© Ù^ÙŠØ³Ù...Ø Ù^Ø·Ù,,ØØ±Ù^Ø± Ø§Ù,,Ø¥Ù^ØªØ±Ù^Øª.
- Ø§Ù,,Ø³Ù...Ø§Ø Ù,,Ø-Ù...ÙŠØ¹ Ù,,Ù^Ø§Ø¹Ù... Ø§Ù,,ØªØÙ^Ù... Ù^ÙŠ Ø§Ù,,Ù^ØµÙ^Ù,, Ø¥Ù,,Ù%Ø§Ù,,Ù^Ù,, (DACL) - ÙŠØ³Ù...Ø Ù,,Ø-Ù...ÙŠØ¹ ØØ±Ù^Ø± Ø§Ù,,Ù...Ø±Ù^Ø± Ù,,ØØ§Ù,,Ø© Ø§Ù,,ØªÙ^Ø§Ù^Ù,, Ù...Ø¹ Ø§Ù,,Ù^Ø±Ø¹.

Downloadable ACL List > PostureNonCompliant1

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content	1234567	permit udp any any eq domain
	8910111	permit ip any host 192.168.15.14
	2131415	permit tcp any any eq 80
	1617181	permit tcp any any eq 443
	9202122	
	2324252	
	6272829	
	3031323	
	3343536	
	3738394	

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic (i)

* DACL Content

1234567	deny ip any 10.0.0.0 255.0.0.0
8910111	deny ip any 172.16.0.0 255.240.0.0
2131415	deny ip any 192.168.0.0 255.255.0.0
1617181	permit ip any any
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic (i)

* DACL Content

123456	permit ip any any
7891011	
121314	
151617	
181920	
212223	
242526	
272829	
303132	
333435	
363738	

▶ Check DACL Syntax

Ø§Ù,,Ø©Ø·Ù^Ø© 12. Ù,Ù... Ø·Ø¥Ù+Ø'Ø§Ø; Ø«Ù,,Ø§Ø«Ø© Ù...Ù,,Ù Ø§Øª ØªØ¹Ø±ÙŠÙ Ø,,Ù,,ØªØ©Ù^ÙŠÙ,, Ù,,Ù,,Ø§Ø±Ù,,Ø§Øª Ø°ÙŠØ± Ù...Ø¹Ø±Ù^Ù Ø© Ù,,Ù,,Ù^Ø¶Ø¹ØÆ Ø°ÙŠØ± Ù...ØªÙ^Ø§Ø±Ù,Ø© Ù...Ø¹ Ø§Ù,,Ù^Ø¶Ø¹ Ù^Ù...ØªÙ^Ø§Ø±Ù,Ø© Ù...Ø¹ Ø§Ù,,Ù^Ø¶Ø¹.

Ù,,Ù,,Ù,,Ù,ÙšØSÙ... Ø"Ø"Ù,,ÙfØÆ ØSÙ†ØªÙ,,Ù,, Ø¥Ù,,Ù% Ø§Ù,,Ø³ÙšØ§Ø³Ø© > Ø¹Ù†Ø§ØØ±
Ø§Ù,,Ø³ÙšØ§Ø³Ø© > Ø§Ù,,Ù†ØªØ§Ø!Ø¬ > Ø§Ù,,ØªÙ ̧Ù^ÙšØ¶ > Ù...Ù,,Ù ̧ØSØª
ØªØ@ØµÙšØµ ØSÙ,,ØªÙ ̧Ù^ÙšØ¶. Ù ̧Ùš Ù...Ù,,Ù ̧ ØSÙ,,ØªØ¹Ø±ÙšÙ ̧ Posture
UnknownØÆ ØØ-Ø Posture Unknown DACLOÆ Ù^Ù ̧ØØµ Ø¥Ø¹Ø§Ø-ØØ ØªÙ-Ø-ÙšÙ‡
Ø§Ù,,Ù^ÙšØ¬ØÆ Ù-ØØ-Ø ØªØ²Ù^ÙšØ- Ø§Ù,,Ø¹Ù...ÙšÙ,,ØÆ Ù^Ù,,Ù... Ø¬ØªÙ^Ù ̧ÙšØ± ØSØ³Ù...
Ù,,ØSØ!Ù...ØØ ØSÙ,,ØªØÙfÙ... Ù ̧Ùš ØSÙ,,Ù^ØµÙ^Ù,, (ACL) Ù,,Ø¥Ø¹ØSØ-ØØ
ØSÙ,,ØªÙ^Ø-ÙšÙ‡ (ØSÙ,,Ø"Ùš ØªÙ... ØªÙfÙ^ÙšÙ†Ù‡ Ø¹Ù,,Ù% FTD)ØÆ Ù^ØØ-Ø-
ØSÙ,,Ø"Ù^ØSØ"ØØ.

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

ACL

Value

▼ Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = url-redirect-acl=fyusifovredirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&acti

Posture DACL

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

DACL Name

▼ Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant

DAACL

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PermitAll

Ø§Ù,,Ø®Ø·Ù^Ø© 13. Ù,Ù... Ø·Ø¥Ù+Ø´Ø§Ø; Ø³ÙŠØ§Ø³Ø§Øª Ø§Ù,,ØªØ®Ù^ÙŠÙ,, ØªØªª
Ø§Ù,,Ø³ÙŠØ§Ø³Ø© > Ù...Ø-Ù...Ù^Ø¹Ø§Øª Ø§Ù,,Ø³ÙŠØ§Ø³Ø§Øª > Ø§Ù,,Ø§Ù ØªªØ±Ø§Ø¶ÙŠ >
Ø³ÙŠØ§Ø³Ø© Ø§Ù,,ØªØ®Ù^ÙŠÙ,, ÙfÙ...Ø§ ÙŠØªÙ... Ø¥Ø³ØªØ®Ø-Ø§Ù... ØØ§Ù,,Ø©
Ù^Ø¶Ù^ÙŠØ© Ø§Ù,,Ø´Ø±Ø· Ù^Ø§Ø³Ù... Ù...Ø-Ù...Ù^Ø¹Ø© Ù†Ù ØÙ, VNP.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Default Default policy set

Authentication Policy (3)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (18)

Status	Rule Name	Conditions	Results
✔	FTD-VPN-Posture-Compliant	AND Session-PostureStatus EQUALS Compliant Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	× PermitAll
✔	FTD-VPN-Posture-NonCompliant	AND Session-PostureStatus EQUALS NonCompliant Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	× FTD-VPN-NonCompliant
✔	FTD-VPN-Posture-Unknown	AND Session-PostureStatus EQUALS Unknown Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	× FTD-VPN-Redirect

Ø§Ù,,ØªØÙ,Ù, Ù...Ù† Ø§Ù,,ØµØ©

Ø§Ø³ØªØ®ØÙ... Ù†ØªØ§ Ø§Ù,,Ù,Ø³Ù... Ù,,ØªØ£ÙfÙšØ- Ø¹Ù...Ù,, Ø§Ù,,ØªÙfÙ`ÙšÙ† Ø·Ø`ÙfÙ,, ØµÙšØ.

Ø¹Ù,,Ù% ISEØœ Ø®Ø·Ù`Ø© Ø§Ù,,ØªØÙ,Ù, Ø§Ù,,Ø£Ù`Ù,,Ù% Ù†Ùš RADIUS Live Log. Ø§Ù†ØªÙ,,Ù,, Ø¥Ù,,Ù% Ø§Ù,,Ø¹Ù...Ù,,ÙšØ§Øª > Ø³Ø-Ù,, RADIUS Live. Ù†Ù†Ø§Øœ Ø§Ù,,Ù...Ø³ØªØ®ØÙ... Ø£Ù,,ÙšØ³ Ù...ØªØµ,, Ù`ÙšØªÙ... ØªØØ-ÙšØ- Ù†Ù†Ø- Ø§Ù,,ØªØ®Ù`ÙšÙ,, Ø§Ù,,Ù...ØªÙ`Ù,Ø¹.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0

Refresh Never

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address
Feb 03, 2020 07:13:31.92...	●	🔒	0	alice@training e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10
Feb 03, 2020 07:13:29.74...	✔	🔒		#ACSACL#-IP-P...						
Feb 03, 2020 07:13:29.73...	✔	🔒		alice@training e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	

Last Updated: Mon Feb 03 2020 08:16:39 GMT+0100 (Central European Standard Time)

0^0^0... 0...0.0\$0^0,00 0^0\$0\$0^00 0\$0,,0^0@0^0\$0,, FTD-VPN-Posture-Unknown000
0^0+0^0\$0-00 0,,0^0,,0f000 0\$0^0... 0\$0±0^0\$0,, FTD-VPN-Profile 0\$0,,0%0 FTD.

Overview

Event	5200 Authentication succeeded
Username	alice@training.example.com
Endpoint Id	00:0C:29:5C:5A:96 ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> FTD-VPN-Posture-Unknown
Authorization Result	FTD-VPN-Redirect

Authentication Details

Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

00\$0,,00 0\$0,,0^0\$0^ 0...0^0,,0,00.

NAS IPv4 Address	192.168.15.15
NAS Port Type	Virtual
Authorization Profile	FTD-VPN-Redirect
Posture Status	Pending
Response Time	365 milliseconds

0\$0,0^0± 0,0^0... 0\$0,,0+0^0\$0:0- 0\$0,,0^0...0\$0^ 0\$0,,0^0\$ 0\$0^0... 0\$0±0^0\$0,,0^0\$ 0\$0,,0%0 FTD.

Result	
Class	CACS:000000000000c0005e37c81a:fyusifov-26-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect
cisco-av-pair	url-redirect=https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=000000000000c0005e37c81a&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp&token=0d90f1cdf40e83039a7ad6a228603112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

VPN sessionDB AnyConnect. ISE (VPN)

<#root>

fyusifov-ftd-64#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : alice@training.example.com

Index : 12

Assigned IP : 172.16.1.10

Public IP : 10.229.16.169

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1

Bytes Tx : 15326 Bytes Rx : 13362

Pkts Tx : 10 Pkts Rx : 49

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Group Policy : DfltGrpPolicy

Tunnel Group : EmployeeVPN

Login Time : 07:13:30 UTC Mon Feb 3 2020

Duration : 0h:06m:43s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : 000000000000c0005e37c81a

Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 12.1
Public IP : 10.229.16.169
Encryption : none Hashing : none
TCP Src Port : 56491 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : win
Client OS Ver: 10.0.18363
Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076

Bytes Tx : 7663 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 12.2
Assigned IP : 172.16.1.10 Public IP : 10.229.16.169
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 56495
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7663 Bytes Rx : 592
Pkts Tx : 5 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

DTLS-Tunnel:

Tunnel ID : 12.3
Assigned IP : 172.16.1.10 Public IP : 10.229.16.169
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 59396
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 0 Bytes Rx : 12770
Pkts Tx : 0 Pkts Rx : 42
Pkts Tx Drop : 0 Pkts Rx Drop : 0

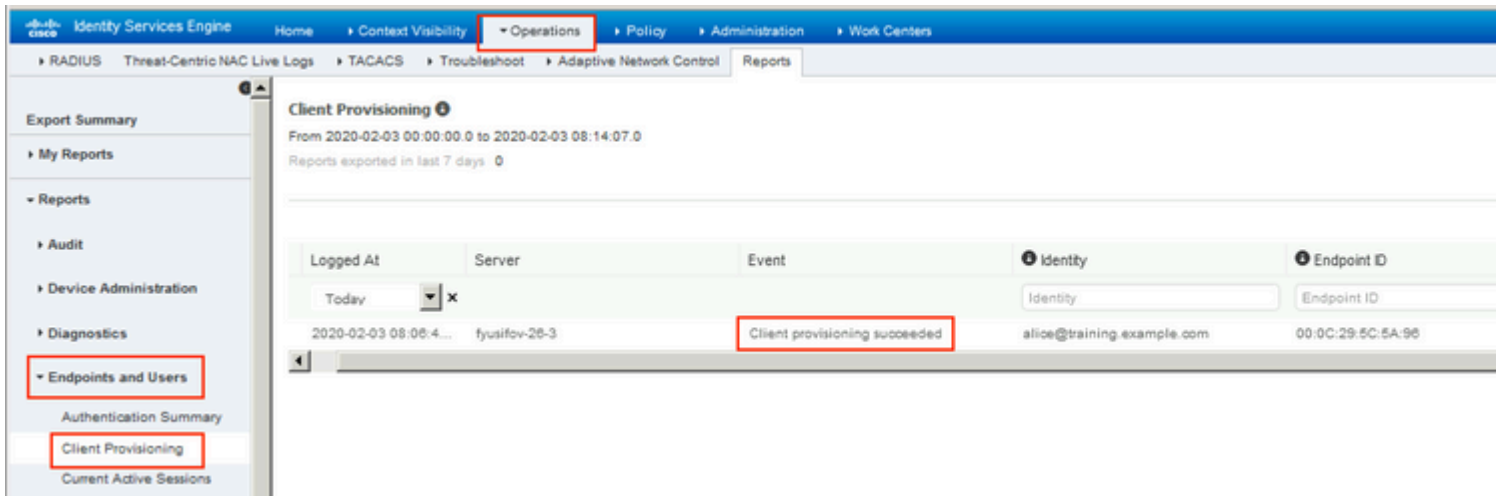
Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture:

Redirect URL : <https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000c0005e37c81>
Redirect ACL : fyusifovredirect

fyusifov-ftd-64#

ÙŠÙ...ÙfÙ† Ø§Ù,,ØªØÙ,Ù, Ù...Ù† Ù†Ù‡Ø¬ ØªØ²ÙˆÙŠØ¬ Ø§Ù,,Ø¹Ù...ÙŠÙ,, Ø§Ù†ØªÙ,Ù,, Ø¥Ù,,Ù%
Ø§Ù,,Ø¹Ù...Ù,,ÙŠØ§Øª > Ø§Ù,,ØªÙ,Ø§Ø±ÙŠØ± > Ù†Ù,Ø§Ø· Ø§Ù,,Ù†Ù‡Ø§ÙŠØ©
ÙˆØ§Ù,,Ù...Ø³ØªØ®Ø-Ù...ÙŠÙ† > Ø¥Ù...Ø-Ø§Ø¬ Ø§Ù,,Ø¹Ù...ÙŠÙ,,.



ÙŠÙ...ÙfÙ† Ø§Ù,,ØªØÙ,Ù, Ù...Ù† "ØªÙ,Ø±ÙŠØ± Ø§Ù,,ÙˆØ¶Ø¹" Ø§Ù,,Ø°ÙŠ ØªÙ... Ø¥Ø±Ø³Ø§Ù,,Ù‡
Ù...Ù† AnyConnect. Ø§Ù†ØªÙ,Ù,, Ø¥Ù,,Ù% Ø§Ù,,Ø¹Ù...Ù,,ÙŠØ§Øª > Ø§Ù,,ØªÙ,Ø§Ø±ÙŠØ± >
Ù†Ù,Ø§Ø· Ø§Ù,,Ù†Ù‡Ø§ÙŠØ© ÙˆØ§Ù,,Ù...Ø³ØªØ®Ø-Ù...ÙŠÙ† > ØªÙ,ÙŠÙŠÙ... Ø§Ù,,ÙˆØ¶Ø¹
Ø³Ø· Ù†Ù,Ø·Ø© Ø§Ù,,Ù†Ù‡Ø§ÙŠØ©.

Export Summary

My Reports

Reports

- Audit
- Device Administration
- Diagnostics
- Endpoints and Users**
 - Authentication Summary
 - Client Provisioning
 - Current Active Sessions
 - External Mobile Device...
 - Manual Certificate Pro...
 - PassiveID
 - Posture Assessment by ...
 - Posture Assessment by ...**

Posture Assessment by Endpo

From 2020-02-03 00:00:00.0 to 2020-02-03 00:00:00.0

Reports exported in last 7 days 0

	Logged At	St
x	Today	x
	2020-02-03 08:07:5...	

øšù,,ù`ø¶ø¹øœ øšù+ù,ø± ùøùù, øªùøšøµùšù,,.

Identity Services Engine	
Posture More Detail Assessment	
From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:36.0	
Generated At: 2020-02-03 08:13:37.37	
Client Details	
Username	alice@
Mac Address	00:0C
IP address	172.1
Location	All Lo
Session ID	00000
Client Operating System	Windo
Client NAC Agent	AnyC
PRA Enforcement	0
CoA	Recei
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEn
System Name	DESK
System Domain	n/a
System User	admin
User Domain	DESKTOP-
AV Installed	
AS Installed	
AM Installed	Windows De

Posture Report	
Posture Status	Compliant
Logged At	2020-02-03 08:07:50.03

Posture Policy Details				
Policy	Name	Enforcement Type	Status	Passed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor

ø·ø¹ø ø¥ø³øªù,,øšù... øšù,,øªù,ø±ùšø± ø¹ù,,ù%ø ISEøœ ùšøªù... øªøø-ùšø« øøšù,,øø øšù,,ù`ø¶ø¹. ùøùù ùøøøøø øšù,,ù...ø«øšù,,øœ øøšù,,øø øšù,,ù`ø¶ø¹ ù...øªù`øšùøùøù,øø ù`ùšøªù... øªøøøøùšù,, øùøø¹ CoA ù...ø¹ ù...ø-ù...ù`ø¹øø ø-øùšøøø ù...ùø øšù,,ø³ù...øøøª.



Refresh



Reset Repeat Counts



Export To ▾

	Time	Status	Details	Rep
✕		<input type="text"/>	▼	
	Feb 03, 2020 08:07:52.05...	✓		
	Feb 03, 2020 08:07:50.03...	ⓘ		0
	Feb 03, 2020 07:13:29.74...	✓		
	Feb 03, 2020 07:13:29.73...	✓		

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Sta

Overview

Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19 ⓘ
Endpoint Profile	
Authorization Result	PermitAll

Authentication Details

Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fysifov-26-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	000000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

◆ ÛŠ ØšÛ,, Û^ØµÛ^Û,, (ACL) ØšÛ,, Ø-Ø ÛŠØ-Ø© Û,, Ø¥Ø¹ØšØ-Ø© ØšÛ,, ØªÛ^Ø-ÛŠÛ‡ Û^Ø¹Û†Û^ØšÛ† URL Û,, Ø¥Ø¹ØšØ-Ø© ØšÛ,, ØªÛ^Ø-ÛŠÛ‡ Û,, Ø-Û,, Ø³Ø© Ø¹Û...Û,, ØšÛ,, Ø´Ø` ÛfØ© ØšÛ,, Ø®ØšØµØ© ØšÛ,, Ø, ØšÛ‡Ø±ÛŠØ© (VPN) Û^Û...Û† ØªØ·Ø` ÛŠÛ, AllowAll DACL.

<#root>

fyusifov-ftd-64#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username :

alice@training.example.com

Index : 14
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 53990 Bytes Rx : 23808
Pkts Tx : 73 Pkts Rx : 120
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

EmployeeVPN

Login Time : 16:58:26 UTC Mon Feb 3 2020
Duration : 0h:02m:24s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000000e0005e385132
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 14.1
Public IP : 10.55.218.19
Encryption : none Hashing : none
TCP Src Port : 51965 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : win
Client OS Ver: 10.0.18363
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7663 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 14.2
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 51970
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7715 Bytes Rx : 10157
Pkts Tx : 6 Pkts Rx : 33
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

DTLS-Tunnel:

Tunnel ID : 14.3
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 51536
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 38612 Bytes Rx : 13651
Pkts Tx : 62 Pkts Rx : 87
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

Ø§Ø³ØªÙfØ´Ø§Ù Ø§Ù,,Ø£Ø®Ø·Ø§Ø; Ù~Ø¥ØµÙ,,Ø§ØÙ±Ø§

ÙšÙ^Ù Ø± Ù±Ø°Ø§ Ø§Ù,,Ù,Ø³Ù... Ù...Ø¹Ù,,Ù^Ù...Ø§Øª ÙšÙ...ÙfÙ†Ùf
Ø¥Ø³ØªØ®Ø¯Ø§Ù...Ù±Ø§ Ù,,Ø§Ø³ØªÙfØ´Ø§Ù Ø£Ø®Ø·Ø§Ø; Ø§Ù,,ØªÙfÙ^ÙšÙ†
Ù^Ø¥ØµÙ,,Ø§ØÙ±Ø§.

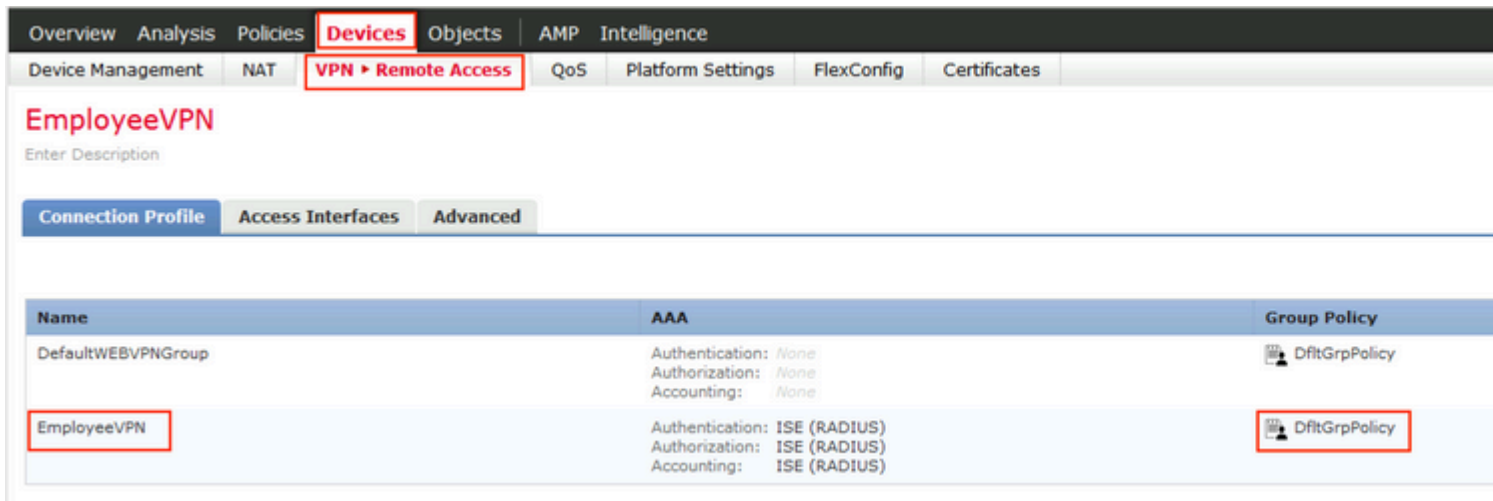
Ù,,Ù,,ØØµ^Ù,, Ø¹Ù,,Ù% ØªØ-Ù ØªÙ...Ù^Ø¶Ø¹ Ù...Ù ØµÙ,, Ù^Ù,,Ø§Ø³ØªÙfØ´Ø§Ù Ø£Ø®Ø·Ø§Ø; AnyConnect Ù^ ISE Ù^Ø¥ØµÙ,,Ø§ØÙ±Ø§Ø£ ØªØÙ,, Ù...Ù† Ù±Ø°Ø§ Ø§Ù,,Ø§Ø±ØªØ¨ Ø§Ø: Ù...Ù,Ø§Ø±Ù†Ø© Ù†Ù...Ø· ISE Posture (Ù^Ø¶Ø¹ÙšØ© Ù...ØØ±Ùf Ø®Ø-Ù...Ø§Øª Ø§Ù,,Ù±Ù^ÙšØ© (ISE)) Ù,,Ù,,pre Ù^ post 2. 2.

- Ù†Ù Ø³Ø§Ù,,Øª

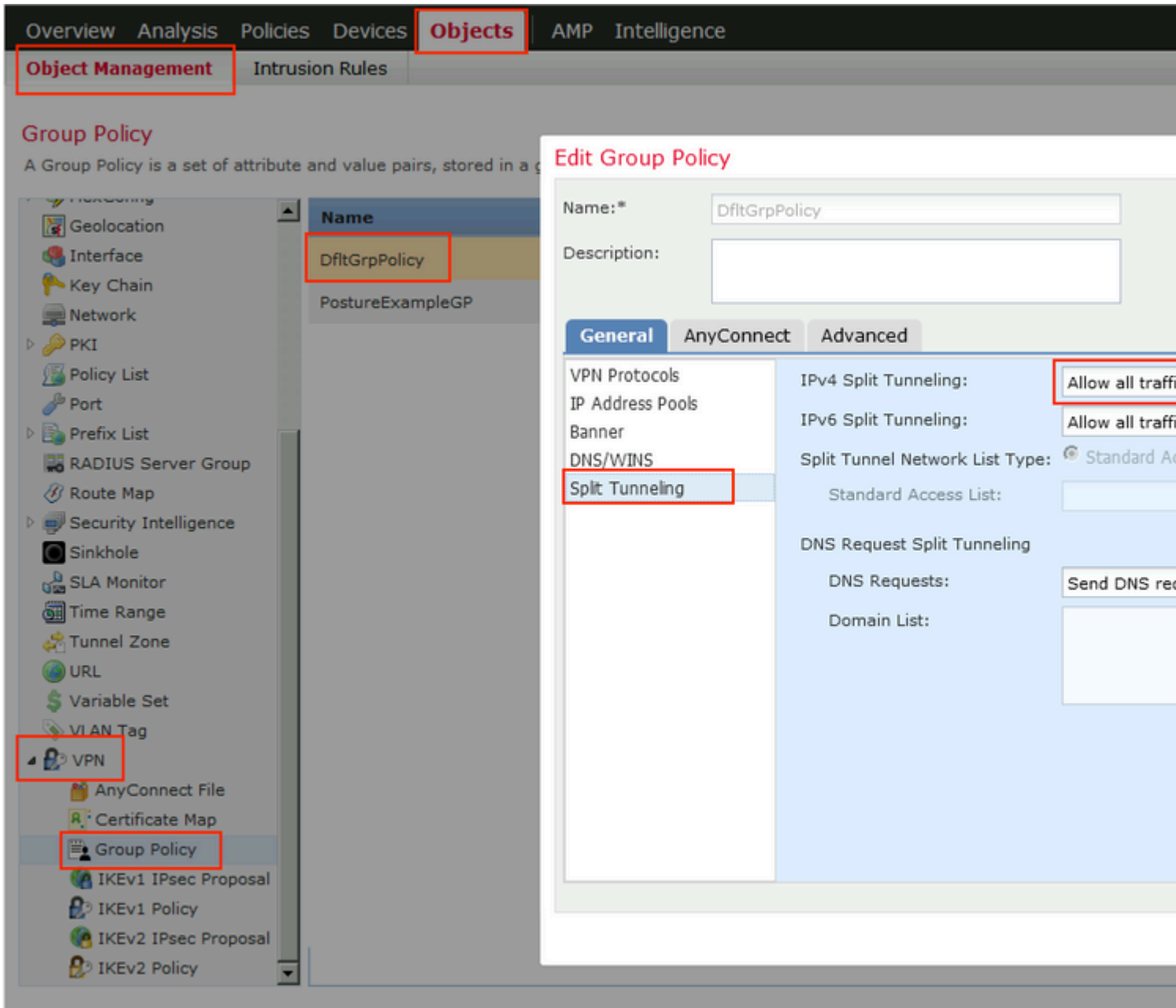
Ø¥ØØ-Ù% Ø§Ù,,Ù...Ø´ÙfÙ,,Ø§Øª Ø§Ù,,Ø´Ø§Ø;Ø¹Ø©Ø£ Ø¹Ù†Ø- ØªÙfÙ^ÙšÙ† Ù†Ù Ø±Ù, spit.
Ù Ùš Ù±Ø°Ø§ Ø§Ù,,Ù...Ø«Ø§Ù,,Ø£ ÙšØªÙ... Ø¥Ø³ØªØ®Ø¯Ø§Ù... Ù†Ù±Ø-
Ø§Ù,,Ù...Ø-Ù...Ù^Ø¹Ø© Ø§Ù,,Ø§Ù ØªØ±Ø§Ø¶ÙšØ£ Ù^Ø§Ù,,Ø°Ùš ÙšÙ†Ù Ø±ÙfØ©
Ù...Ø±Ù^Ø± Ø§Ù,,Ø¨ ÙšØ§Ù†Ø§Øª Ø¨ Ø§Ù,,ÙfØ§Ù...Ù,, Ù Ùš Ø§Ù,, Ø¥Ù†Ø´Ø§Ø;

Ù,Ù+Ù^Ø§Øª Ù,,ØØ±ÙfØ© Ù...Ø±Ù^Ø± Ù...Ø¹ÙŠÙ+Ø© Ù◆Ù,Ø·Øœ Ù◆ÙŠØ-Ø" Ø£Ù†
 ØªÙ...Ø± Ù...Ø³ØªÙfØ´Ù◆Ø§Øª AnyConnect (enroll.cisco.com Ù^Ù...Ø¶ÙŠÙ◆
 Ø§Ù,,Ø§ÙfØªØ´Ø§Ù◆) Ø¹Ø" Ø± Ø§Ù,,Ù†Ù◆Ù, Ø"Ø§Ù,,Ø¥Ø¶Ø§Ù◆Ø© Ø¥Ù,,Ù% ØØ±ÙfØ©
 Ù...Ø±Ù^Ø± Ø§Ù,,Ø"ÙŠØ§Ù+Ø§Øª Ø¥Ù,,Ù% ISE Ù^Ø§Ù,,Ù...Ù^Ø§Ø±Ø¯ Ø§Ù,,Ø¯Ø§Ø®Ù,,ÙŠØ©
 Ø§Ù,,Ø£Ø®Ø±Ù%.

Ù,,Ù,,ØªØÙ,Ù, Ù...Ù† Ø³ÙŠØ§Ø³Ø© Ø§Ù,,Ù†Ù◆Ù, Ø¹Ù,,Ù% FMCØœ Ø£Ù^Ù,,Ø§Øœ
 Ø§Ù,,ØªØÙ,Ù, Ù...Ù† Ù†Ù‡Ø¬ Ø§Ù,,Ù...Ø-Ù...Ù^Ø¹Ø© Ø§Ù,,Ø°ÙŠ ÙŠØªÙ...
 Ø¥Ø³ØªØ®Ø¯Ø§Ù...Ù‡ Ù,,Ø§ØªØµØ§Ù,, VPN. Ø§Ù†ØªÙ,,Ù, Ø¥Ù,,Ù% Ø§Ù,,Ø£Ø-Ù‡Ø²Ø© >
 Ø§Ù,,Ù^Øµ^Ù,, Ø¹Ù† Ø"Ø¹Ø- Ø¥Ù,,Ù% VPN.



Ø"Ø¹Ø- Ø°Ù,,ÙfØœ Ø§Ù†ØªÙ,,Ù,, Ø¥Ù,,Ù% Ø§Ù,,ÙfØ§Ø!Ù†Ø§Øª > Ø¥Ø-Ø§Ø±Ø©
 Ø§Ù,,ÙfØ§Ø!Ù† > VPN > Ù†Ù‡Ø¬ Ø§Ù,,Ù...Ø-Ù...Ù^Ø¹Ø© Ù^Ø§Ù†Ù,Ø± Ù◆Ù^Ù, Ù†Ù‡Ø¬
 Ø§Ù,,Ù...Ø-Ù...Ù^Ø¹Ø© Ø§Ù,,Ø°ÙŠ ØªÙ... ØªÙfÙ^ÙŠÙ†Ù‡ Ù,,Ù,,Ø"Ø´ÙfØ© Ø§Ù,,Ø®Ø§Ø®Ø©
 Ø§Ù,,Ø,Ø§Ù‡Ø±ÙŠØ© (VPN).



- Identity NAT

nat (inside) 100 10.10.10.0/24 10.10.10.0/24
 nat (inside) 101 10.10.10.0/24 10.10.10.0/24
 nat (inside) 102 10.10.10.0/24 10.10.10.0/24

nat (inside) 103 10.10.10.0/24 10.10.10.0/24
 nat (inside) 104 10.10.10.0/24 10.10.10.0/24
 nat (inside) 105 10.10.10.0/24 10.10.10.0/24

Overview

Analysis

Policies

Devices

Objects

Device Management

NAT

VPN ▼


QoS

Plat

FTD_11

Enter Description

Rules

 Filter by Device

#	Direction	Type	Source Interface Ob...	Destina Interfa
---	-----------	------	------------------------	-----------------

▼ NAT Rules Before

1. Rule 1: NAT Rule Before
 Direction: Outgoing
 Type: NAT
 Source Interface: Any
 Destination Interface: Any

Edit NAT Rule

NAT Rule:

Manual NAT Rule

Type:

Static

Enabled

Description:

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Original Source:*

any

Original Destination:

Address

VPN_Subnet

Original Source Port:

Original Destination Port:

0^0^ 0^ù,,0\$ù...0© 0\$ù,,0^0^·ù^ùš0^ 0@ùš0\$0±0\$0^ ù...0^ù,0^ù...0©0E 00^0^ 0@0\$ù^0\$0^ 0\$ù,,0\$0@0^ùš0\$0± ùfù...0\$ ù‡ù^ ù...ù^0¶0 ù◆ùš ù‡0°ù‡ 0\$ù,,0μù^0±0©:

Edit NAT Rule

NAT Rule:

Insert:

Type:

Enable

Description:

Interface Objects

Translation

PAT Pool

Advanced

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا