Risoluzione dei problemi relativi alle distribuzioni dei criteri di difesa dalle minacce Firepower

Sommario

Introduzione

Con Cisco Firepower Threat Defense (FTD), le tradizionali funzionalità del firewall di tipo stateful offerte dalle appliance ASA (Adaptive Security Appliance) e dalle funzionalità del firewall di nuova generazione (con tecnologia Snort) sono ora integrate in un unico prodotto. A causa di questa modifica, Policy Deployment Infrastructure su FTD ora gestisce le modifiche alla configurazione sia per il codice ASA (noto anche come LINA) che per lo snort in un bundle. Questo documento fornisce una panoramica di alto livello del processo di distribuzione delle policy su FTD e delle tecniche di risoluzione dei problemi di base.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Avviso: Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica sulla distribuzione dei criteri

Cisco FTD utilizza le distribuzioni di policy per gestire ed eseguire il push delle configurazioni dei dispositivi registrati nel Firepower Management Center (FMC) stesso. All'interno dell'implementazione, sono presenti una serie di passaggi suddivisi in "Fasi".

Le fasi del CCP possono essere riassunte nel seguente elenco.

Fase 0	Inizializzazione distribuzione
Fase 1	Raccolta oggetti di database
Fase 2	Raccolta oggetti e criteri
Fase 3	Generazione della configurazione dalla riga di comando NGFW
Fase 4	Generazione del pacchetto di distribuzione del dispositivo
Fase 5	Invio e ricezione del pacchetto di distribuzione
Fase 6	Messaggi di distribuzione, azioni di distribuzione e completamento distribuzione in sospeso

La comprensione delle fasi e la conoscenza della posizione del guasto nel processo possono essere utili per la risoluzione dei problemi che un sistema Firepower deve affrontare. In alcune situazioni, potrebbe trattarsi di un conflitto causato da configurazioni precedenti o da una parola chiave mancante in Advanced Flex Configuration che può causare errori per i quali il report del dispositivo non è esplicito.

Panoramica di esempio

Passaggio 1. L'utente fa clic sul pulsante "Distribuzione", specificando quale dispositivo desidera selezionare.

Passaggio 2. Dopo il commit della distribuzione di un dispositivo, il CCP inizia a raccogliere tutte le configurazioni relative al dispositivo.

Passaggio 3. Una volta raccolte le configurazioni, la FMC crea il pacchetto e lo invia al sensore tramite il meccanismo di comunicazione denominato SFTunnel.

Passaggio 4. Il CCP notifica quindi al sensore di avviare il processo di installazione utilizzando la policy fornita, ascoltando le singole risposte.

Passaggio 5. Il dispositivo gestito decomprime l'archivio e inizia ad applicare le singole configurazioni e pacchetti.

R. La prima metà dell'implementazione è la configurazione Snort, in cui la configurazione Snort viene testata localmente per garantirne la validità. Una volta dimostrata la validità della nuova configurazione, questa viene spostata nella directory di produzione di Snort. Se la convalida ha esito negativo, la distribuzione dei criteri non riesce in questa fase.

B. La seconda metà del caricamento del pacchetto di installazione è per la configurazione LINA, dove viene applicata direttamente al processo LINA dal processo ngfwManager. Se si verifica un errore, viene eseguito il rollback delle modifiche e si verifica un errore di distribuzione dei criteri.

Passaggio 6. Se entrambi i pacchetti Snort e LINA hanno esito positivo, il dispositivo gestito segnala Snort di riavviare o ricaricare per caricare la nuova configurazione e salvare tutte le configurazioni correnti.

Passaggio 7. Se tutti i messaggi hanno esito positivo, il sensore invia un messaggio di operazione riuscita e attende che venga riconosciuto dal centro di gestione.

Passaggio 8. Una volta ricevuto, il CCP contrassegna l'attività come riuscita e consente il completamento del pacchetto di criteri.

Risoluzione dei problemi

I problemi rilevati durante la distribuzione dei criteri possono essere dovuti, ma non limitati, ai motivi seguenti:

1. Configurazione errata
2. Comunicazione tra CCP e FTD
3. Integrità del database e del sistema
4. Difetti e avvertenze software
5. Altre situazioni uniche

Alcuni di questi problemi possono essere risolti facilmente, mentre altri possono richiedere assistenza al Cisco Technical Assistance Center (TAC).

L'obiettivo di questa sezione è fornire strumenti e tecniche per la risoluzione dei problemi in modo da isolare il problema o determinarne la causa principale.

Risoluzione dei problemi relativi all'interfaccia grafica dell'utente (GUI) di FMC

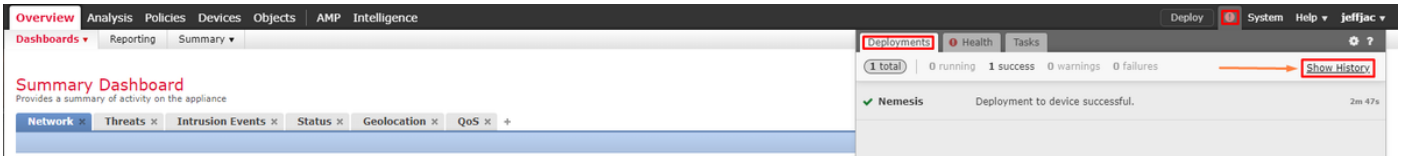
Cisco consiglia di avviare ogni sessione di risoluzione dei problemi per gli errori di distribuzione sull'accessorio FMC.

Nella finestra di notifica degli errori, in tutte le versioni successive alla 6.2.3, sono disponibili ulteriori strumenti di risoluzione dei problemi che possono essere utili in caso di errori.

Utilizzo Delle Trascrizioni Di Distribuzione

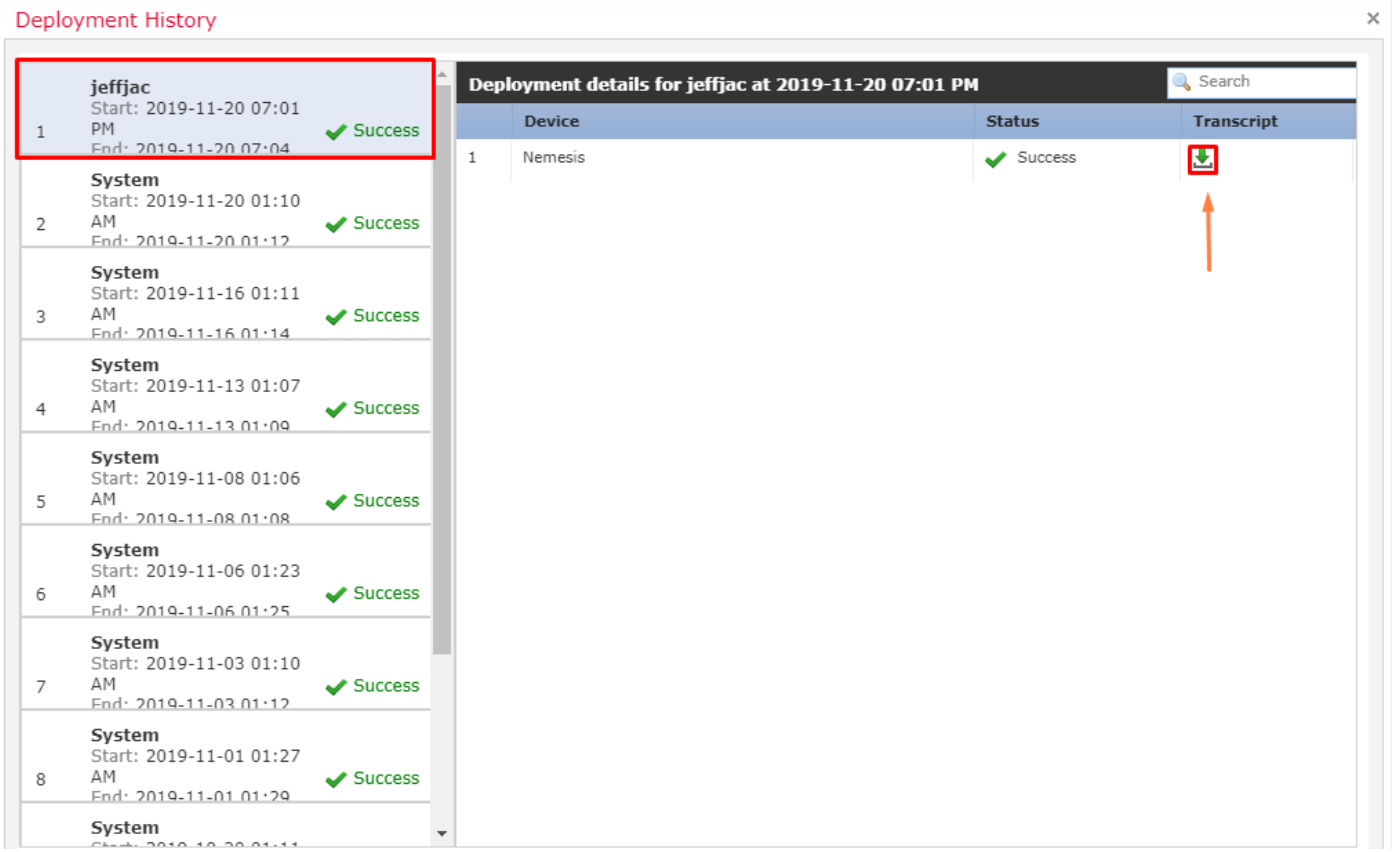
Passaggio 1. Estrarre l'elenco Distribuzioni nell'interfaccia utente Web di FMC.

Passaggio 2. Quando la scheda Distribuzioni è selezionata, selezionare l'opzione "Mostra cronologia".

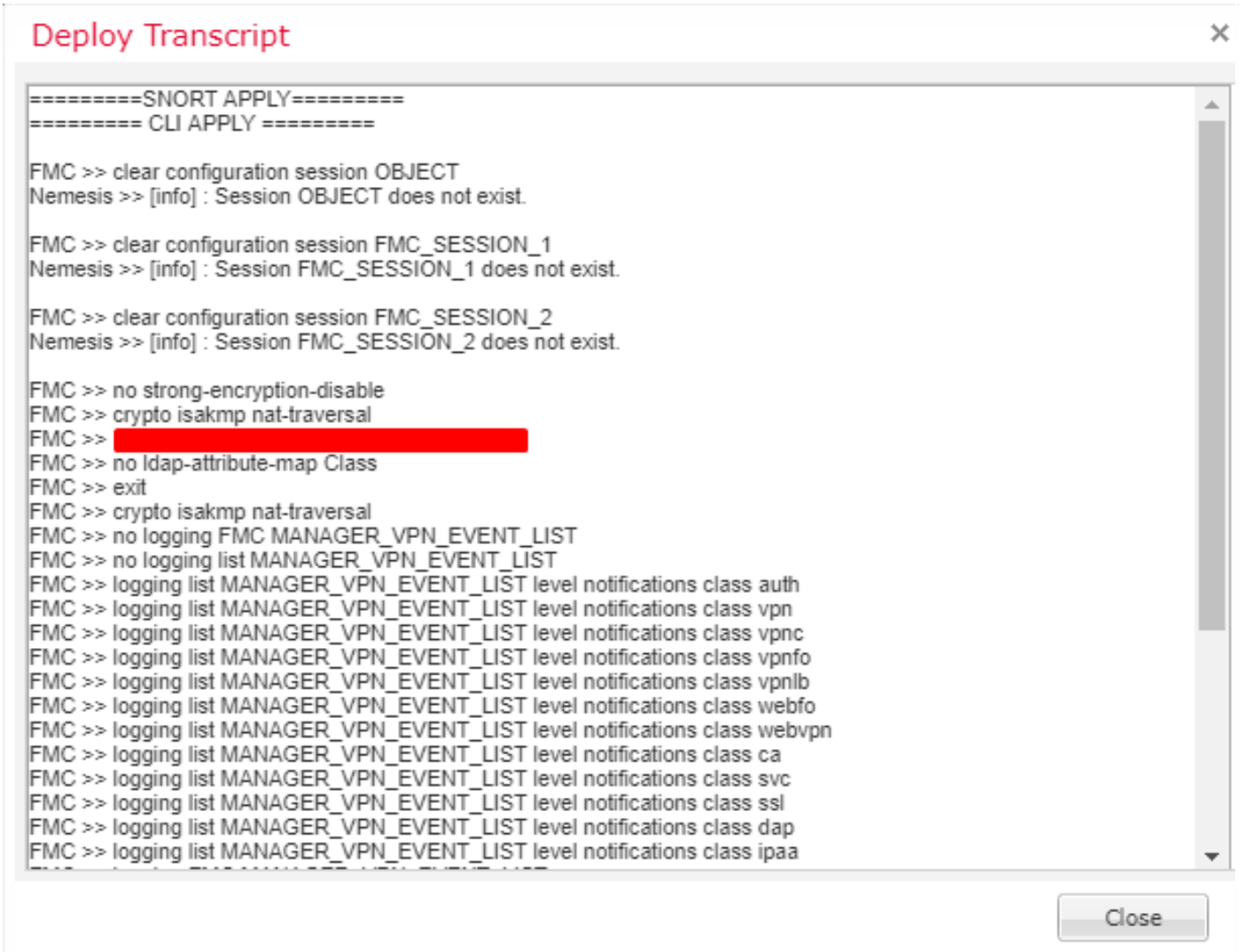


Passaggio 3. Nella casella Cronologia distribuzione è possibile visualizzare tutte le distribuzioni precedenti del CCP. Selezionare la distribuzione in cui si desidera visualizzare ulteriori dati.

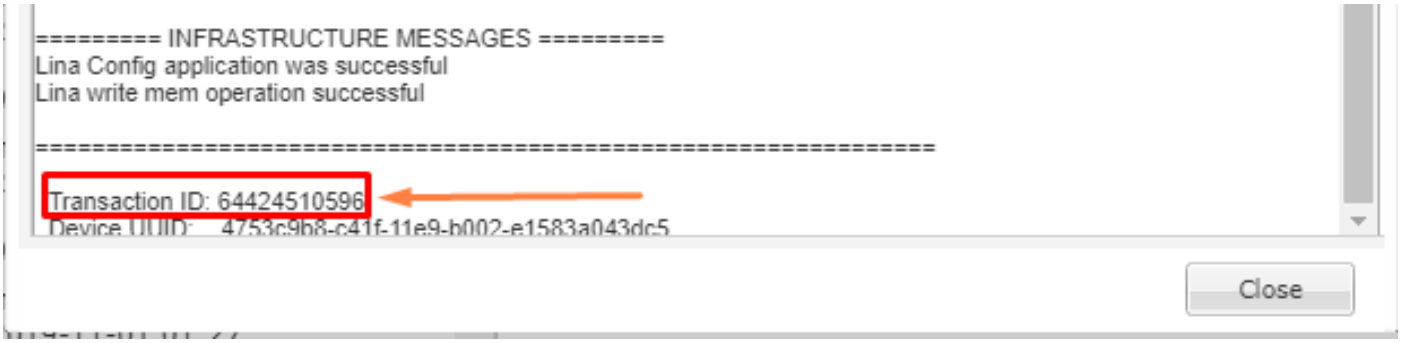
Passaggio 4. Dopo aver selezionato un elemento di distribuzione, viene visualizzata la selezione Dettagli distribuzione che mostra una lista di tutti i dispositivi all'interno della transazione. Queste voci sono suddivise nelle seguenti colonne: Numero dispositivo, Nome dispositivo, Stato e Trascrizione.



Passaggio 5. È possibile selezionare il dispositivo in questione e fare clic sull'opzione di trascrizione per visualizzare la trascrizione della distribuzione individuale che può informare l'utente di errori e configurazioni inserite sui dispositivi gestiti.



Passaggio 6. Questa trascrizione può indicare alcune condizioni di errore e indicare un numero molto importante per il passaggio successivo: ID transazione.



Passaggio 7. In una distribuzione Firepower, l'ID transazione è quello che può essere utilizzato per tenere traccia di ogni singola sezione di una distribuzione di criteri. In questo modo, dalla riga di comando del dispositivo è possibile ottenere una versione più dettagliata di questi dati per la risoluzione dei problemi e l'analisi.

> **Suggerimento**: Se non è possibile individuare l'ID della transazione o se si utilizza una versione precedente alla stampa, è possibile utilizzare il registro precedente per individuare i singoli messaggi di errore.

Risoluzione dei problemi mediante i registri FMC

Anche se è opportuno incaricare Cisco TAC di analizzare i registri, esaminare i registri può contribuire all'isolamento iniziale del problema e accelerare la risoluzione. In FMC sono presenti più file di registro che rivelano i dettagli relativi al processo di distribuzione dei criteri. I due registri di riferimento più comuni sono policy_deployment.log e usmsharedsvcs.log.

Tutti i file menzionati in questo documento possono essere visualizzati con più comandi Linux, come more, less e vi. Tuttavia, è molto importante garantire che vengano eseguite solo azioni di lettura. Per visualizzare tutti i file è necessario l'accesso alla directory principale.

/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

Questo registro indica chiaramente l'inizio dell'attività di distribuzione dei criteri in FMC e il completamento di ogni fase, che consente di determinare la fase in cui la distribuzione è stata interrotta, insieme al codice di errore. Il valore "transactionID" incluso nella parte JSON del log può essere utilizzato per trovare le voci di log relative a un particolare tentativo di distribuzione.

```
22-Nov-2019 01:28:52.844,[INFO],(DefenseCenterServiceImpl.java:1372)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-4
** REST Request [ CSM ]
** ID : e1c84364-0966-42eb-9356-d2914be2b4a3
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:deployment_initiated_for_the_device",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-0"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "running",
  "progress" : 5,
  "silent" : true,
  "restart" : true,
  "transactionId" : 12884916552,
  "devices" : [ "93a2089a-fa82-11e9-8219-e1abeec81dc9" ]
}
```

/var/log/sf/policy_deployment.log

Anche se questo file di log è presente in tutte le versioni 6.x, a partire dalla versione 6.4, la sua copertura è stata ampliata. Viene ora descritta in dettaglio la procedura adottata da FMC per creare i pacchetti di distribuzione, pertanto è consigliabile utilizzarlo per analizzare gli errori della fase 1 - 4. L'inizio di ogni fase è contrassegnato da una riga con "INFO Starting XYZ":

```
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO starting populateGlobalSnapshot -
sqlite = /var/cisco/umpd/8589938337/DC_policy_deployment.db, transaction = 8589938337, time =
1563470402, running as (memory = 56.35 MB) (Framework 3950<196 <- CSMTasks 223<10 <-
SF::ActionQueue 2457)
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO deployment threading: disabled
(Framework 198 <- CSMTasks 223<10 <- SF::ActionQueue 2457)
```

```
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO -> calling
SF::UMPD::Plugins::Correlation::Manager::getPluginDependencies (Plugin 298<90 <- Framework
3579<3566<216 <- CSMTasks 223)
...
```

Risoluzione dei problemi dei dispositivi gestiti

Sono disponibili ulteriori fasi e sezioni a seconda del pacchetto del dispositivo, della configurazione ad alta disponibilità e del risultato delle fasi precedenti per ciascun dispositivo gestito. Se un problema di distribuzione è isolato a un errore sul dispositivo gestito, è possibile eseguire ulteriori operazioni di risoluzione dei problemi sul dispositivo utilizzando due registri sul dispositivo: policy_deployment.log e ngfwManager.log.

/ngfw/var/log/ngfwManager.log

In questo file di log vengono illustrati in dettaglio i passaggi eseguiti da Config Communication Manager e Config Dispatcher per comunicare con FMC, utilizzare il pacchetto di distribuzione e orchestrare la convalida e l'applicazione delle configurazioni Snort e LINA. Ecco alcuni esempi di ngfwManager.log che rappresentano l'inizio delle fasi principali:

```
FTD receives FMC's request for running configuration:

May 30 16:37:10 ccm[4293] Thread-10: INFO  com.cisco.ccm.ConfigCommunicationManager- Passing CD-
Message-Request to Config Dispatcher...
May 30 16:37:10 ccm[4293] Thread-10: DEBUG com.cisco.ccm.ConfigCommunicationManager- <?xml
version="1.0" encoding="UTF-
8"?><cdMessagesList><timeStamp>1559234230012</timeStamp><cdMessage><name>LinaShowCommand</name><
messageId>-
7531335374431513 90</messageId><contentType>XML</contentType><msgContent><![CDATA[<?xml
version="1.0" encoding="UTF-8"?><message><name>LinaShowCommand</name>...



FTD receives FMC's request to download the deployment package:

May 30 16:37:18 ccm[4293] Thread-9: INFO  com.cisco.ccm.ConfigCommunicationManager- Downloading
database (transaction 8589938211, version 1559234236)
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- handle record:
8589938211, status = PENDING
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- begin downloading
database



FTD begins the deployment of policy changes:

May 30 16:37:21 ccm[4293] Thread-9: INFO  com.cisco.ccm.ConfigCommunicationManager- Starting
deployment
May 30 16:37:21 ccm[4293] Thread-11: INFO  com.cisco.ccm.ConfigCommunicationManager- Sending
message: DEPLOYMENT_STATUS_CCM to Manager



FTD begins LINA deployment:

May 30 16:37:42 ccm[4293] Thread-19: DEBUG
com.cisco.ngfw.configdispatcher.communicators.LinaCommunicatorImpl- Trying to send Start-Config-
Sequencerequest to lina
```

```
FTD begins finalizing the deployment:

May 30 16:38:48 ccm[4293] Thread-19: DEBUG
com.cisco.ngfw.configdispatcher.communicators.LinaCommunicatorImpl- Clustering Message sent out
of ConfigDispatcher:
Name:Cluster-App-Conf-Finalize-Request
```

/ngfw/var/log/sf/policy_deployment.log

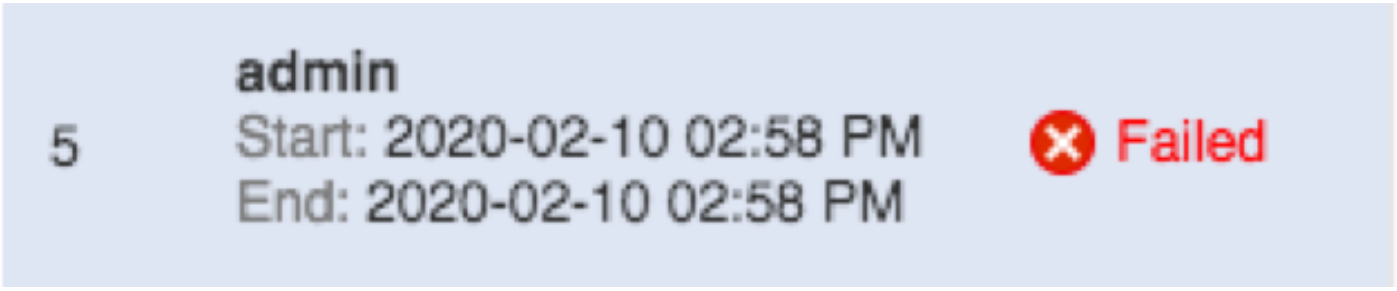
Questo registro contiene i dettagli del criterio applicato a Snort. Sebbene il contenuto del registro sia per lo più avanzato e richieda un'analisi tramite TAC, è comunque possibile tracciare il processo utilizzando alcune voci chiave:

```
Config Dispatcher begins extracting the packaged policies for validation:

Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO  -> calling
SF::UMPD::Plugins::NGFWPolicy::Device::exportDeviceSnapshotToSandbox  (Plugin 230 <- Framework
611 <- Transaction 1085)
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO  found NGFWPolicy =>   (NGFWPolicy::Util
32 <- NGFWPolicy::Device 43 <- Plugin 235)
...
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO export FTD platform settings...
(PlatformSettings::FTD::Device 29 <- Plugin 235<339 <- PlatformSettings::Device 13)



Config validation begins:

Jul 18 17:21:37 firepower policy_apply.pl[25122]: INFO  starting validateExportedFiles - sqlite
= /var/cisco/deploy/sandbox/policy_deployment.db, sandbox = /var/cisco/deploy/sandbox/exported-
files (memory = 229.99 MB)  (Framework 3950<687 <- Transaction 1101 <- main 194)



Validation has completed successfully:

Jul 18 17:21:49 firepower policy_apply.pl[25122]: INFO validateExportedFiles - sqlite =
/var/cisco/deploy/sandbox/policy_deployment.db, sandbox = /var/cisco/deploy/sandbox/exported-
files took 12 (memory = 238.50 MB, change = 8.51 MB) (Framework 3976<724 <- Transaction 1101 <-
main 194)



Config Dispatcher begins moving the validated configuration to the Snort directories in
production:

Jul 18 17:21:54 firepower policy_apply.pl[26571]: INFO  -> calling
SF::UMPD::Plugins::NGFWPolicy::Device::publishExportedFiles  (Plugin 230 <- Framework 822 <-
Transaction 1662)



Snort processes will reload to apply the new configurations:

Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO  Reconfiguring DE a3bcd340-992f-11e9-
a1f1-ac829f31a4f9...  (Snort::SnortNotifications 292<154 <- Snort::Device 343 <- Plugin 235)
Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO  sending SnortReload to a3bcd340-992f-
11e9-a1f1-ac829f31a4f9  (Snort::SnortNotifications 298<154 <- Snort::Device 343 <- Plugin 235)
```

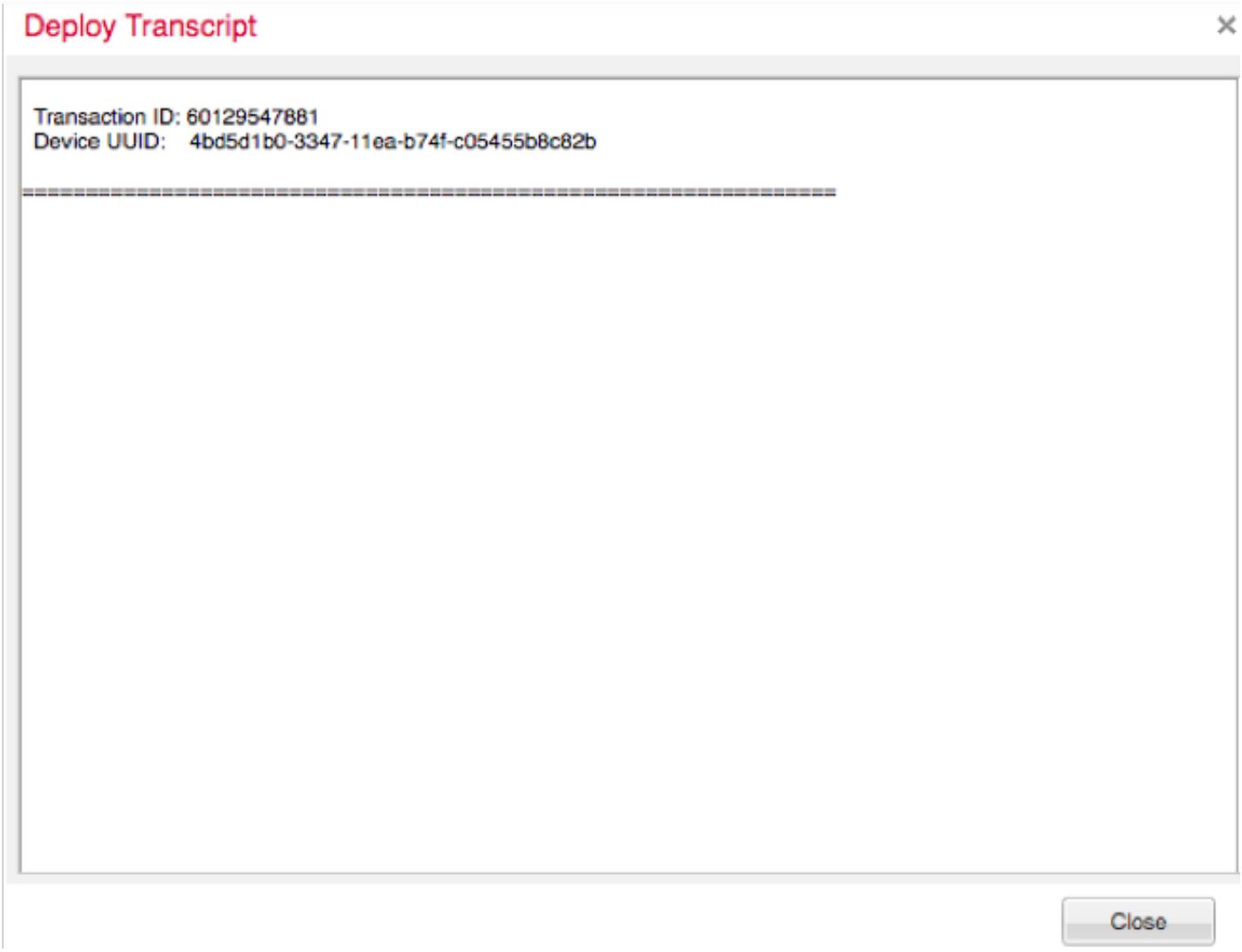
```
Snort reload has completed successfully:

Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox =
/var/cisco/deploy/sandbox/exported-files took 16 (memory = 169.52 MB, change = 16.95 MB)
(Framework 3976<964 <- Transaction 1680 <- main 200)


After LINA config apply finishes, Snort deployment is finalized:

Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO  starting finalizeDeviceDeployment -
sandbox = /var/cisco/deploy/sandbox (memory = 101.14 MB)  (Framework 3950<980 <- Transaction
1740 <- main 206)
```

Esempio

Passaggio 1. Una distribuzione non riesce



Passaggio 2. Ottenere la distribuzione della trascrizione e l'ID transazione.



Passaggio 3. SSH nel centro di gestione e utilizzare meno l'utility Linux per leggere il file come indicato di seguito sul FMC:

Esempio:*"sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log" (la password sudo è la password dell'utente per ssh)*

```
admin@firepower:~$ sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
Password:
```

Passaggio 4. Dopo avere eseguito un numero inferiore di operazioni, utilizzare la barra e immettere l'ID del messaggio per cercare i log relativi all'ID della transazione di distribuzione.

Esempio:*"/60129547881" {In meno, utilizzare n per passare al risultato successivo}*

Esempio di messaggio in esecuzione:

```
10-Feb-2020 19:58:35.810,[INFO],(DefenseCenterServiceImpl.java:1394)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, Thread-526
** REST Request [ CSM ]
** ID : b1b660d2-6c1e-40a0-bbc4-feac62673cc8
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:domain_snapshot_success",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-2"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "running",
  "progress" : 20,
  "silent" : true,
  "restart" : false,
  "transactionId" : 60129547881,
  "devices" : [ "4bd5d1b0-3347-11ea-b74f-c05455b8c82b" ]
}
```

Esempio di messaggio di errore:

```
10-Feb-2020 19:58:36.516,[INFO],(DefenseCenterServiceImpl.java:1394)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, Thread-526
** REST Request [ CSM ]
** ID : 3df80a13-2da8-4eb1-a599-c123bf48ac9f
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:failed_to_retrieve_running_configuration",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-3"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "failure",
  "progress" : 100,
  "silent" : false,
  "restart" : false,
  "transactionId" : 60129547881,
  "devices" : [ "4bd5d1b0-3347-11ea-b74f-c05455b8c82b" ]
}
```

5) Confrontare l'errore corretto con la tabella allegata dei messaggi di errore comuni.

Ad esempio, failed_to_retrieve_running_configuration si verifica durante errori di comunicazione

tra i due dispositivi.

Messaggi di errore comuni

Di seguito sono riportati i messaggi di errore comuni che è possibile visualizzare sul front-end dell'attività del centro di gestione, nonché il codice di errore che può essere visualizzato nel back-end. Questi messaggi possono essere analizzati e confrontati con i motivi comuni per possibili risoluzioni.

Nel caso in cui non vengano visualizzate, o non risolvano la situazione che si sta verificando, contattare TAC per assistenza.

Codice di errore	Messaggi di errore	Motivo
dominio_modificato_dispositivo	Errore di distribuzione. Il dispositivo ha modificato il dominio da{SRCDOMAIN} a {DESTINATIONDOMAIN}. Riprova più tardi.	Questo errore si verifica in genere quando una periferica è in movimento o è in fase di acquisizione da un secondo dominio. Una ridistribuzione in assenza di informazioni tra domini in genere consente di risolvere il problema.
device_current_under_deployment	Distribuzione non riuscita a causa di un'altra distribuzione in corso per questo dispositivo. Riprova più tardi.	Questo viene in genere segnalato quando la distribuzione viene attivata su un dispositivo in fase di distribuzione. In alcune versioni ciò è possibile senza notifica di errore; tuttavia, questa fase esiste ancora per l'assistenza

		nella risoluzione dei problemi.
dispositivo_non_membro_del_contenitore	Impossibile eseguire la distribuzione su un singolo dispositivo membro di un cluster. Riprovare più tardi, distribuendo il cluster.	Questo messaggio è valido per FTD su dispositivi con Firepower eXtensible Operative System (FXOS) Chassis Manager. Questo messaggio viene visualizzato se il cluster è basato su FXOS, ma non su FMC. Creare il cluster sull'accessorio di Management Center prima di tentare la distribuzione.
policy_altered_after_timestamp_for_other_devices_in_job_error	I criteri per uno o più dispositivi sono stati modificati dopo {TIMESTAMP}. Riprovare la distribuzione.	Questo errore viene visualizzato se un criterio o un oggetto viene modificato per un dispositivo nel processo di distribuzione dopo l'attivazione

		dell'utente e prima della creazione degli elementi CSM e degli snapshot del dominio. La ridistribuzione consente di risolvere il problema. Questa situazione può verificarsi quando molti utenti utilizzano gli stessi oggetti di modifica FMC e salvano il file mentre si esegue la distribuzione.
policy_altered_after_timestamp_error	Il criterio {Policy Name} è stato modificato dopo il {Timestamp}. Riprovare la distribuzione.	Questo errore viene visualizzato se un criterio o un oggetto viene modificato per il dispositivo interessato nel processo di distribuzione, dopo l'attivazione dell'utente e prima della creazione di snapshot di dominio e CSM. La ridistribuzione consente di risolvere il problema.
errore_snapshot_csm	Distribuzione non riuscita a causa di un errore nella raccolta di criteri e oggetti. Se il problema persiste, contattare Cisco TAC.	Se viene fornita un'importazione di criteri

		recente, attendere un'ora circa e tentare un'altra distribuzione. Se ciò non consente di procedere, contattare TAC poiché si tratta di un messaggio relativo a un database. Per impostazione predefinita, lo snapshot del dominio ha un timeout di 5 minuti. Se il sistema è sottoposto a un carico elevato, l'hypervisor non funziona correttamente o è sotto carico per un sistema virtuale, ciò può causare ritardi innaturali nella chiamata. Ciò può verificarsi se non viene fornita la quantità corretta di risorse di memoria anche al centro di gestione o al dispositivo. Se il problema
timeout_snapshot_dominio	Distribuzione non riuscita a causa di un timeout durante la raccolta di criteri e oggetti. Se il problema persiste, contattare Cisco TAC.	

		persiste o non viene risolto in un secondo momento, contattare TAC.
errori_snapshot_dominio	Distribuzione non riuscita nella raccolta di criteri e oggetti. Se il problema persiste, contattare Cisco TAC.	Contatta TAC. È necessaria una risoluzione avanzata dei problemi.
failed_to_retrieve_running_configuration	Distribuzione non riuscita a causa di un errore durante il recupero delle informazioni di configurazione in esecuzione dal dispositivo. Riprovare la distribuzione.	Questo messaggio può essere visualizzato quando la connettività tra un sensore terminale e un FMC non funziona come previsto. Verificare lo stato del tunnel tra le unità e monitorare la connettività tra i due dispositivi. Se il tunnel funziona come previsto e i dispositivi possono comunicare,

		contattare TAC.
dispositivo_occupato	Distribuzione non riuscita. È possibile che il dispositivo esegua una distribuzione o un riavvio precedente. Se il problema persiste, contattare Cisco TAC.	Questo messaggio viene visualizzato quando FMC tenta di eseguire una distribuzione mentre è in corso una distribuzione precedente su FTD. Generalmente si verifica quando una distribuzione precedente non è completata su FTD e il FTD viene riavviato o il processo ngfwManager su FTD viene riavviato. Per risolvere il problema, riprovare dopo 20 minuti per consentire il timeout formale dei processi. Se dopo un

		ritardo o se il ritardo non è accettabile, contattare TAC.
no_response_for_show_cmd	Distribuzione non riuscita a causa di problemi di connettività con il dispositivo o il dispositivo non risponde. Se il problema persiste, contattare Cisco TAC.	FMC emette alcuni comandi LINA "show" per recuperare la configurazione in esecuzione per la generazione della configurazione. Questo può accadere quando ci sono problemi di connettività o problemi con il processo ngfwManager sul sensore terminale. Se non si verificano problemi di connettività tra le unità, contattare TAC.
network_latency_or_device_not_reachable	Distribuzione non riuscita a causa di un errore di comunicazione con il	Generalmente si verifica

	dispositivo. Se il problema persiste, contattare Cisco TAC.	con una latenza di rete elevata tra i dispositivi che causa un timeout dei criteri. Verificare la latenza di rete tra i dispositivi per verificare che corrisponda ai valori minimi per la versione indicata nel manuale dell'utente.
slave_app_sync	Distribuzione non riuscita perché è in corso la sincronizzazione della configurazione del cluster. Riprovare la distribuzione.	Questa opzione è applicabile solo per le impostazioni cluster FTD. Se si tenta una distribuzione in un cluster FTD mentre è in corso la sincronizzazione dell'app (sincronizzazione della configurazione), la stessa operazione viene rifiutata da FTD. Per risolvere il problema, riprovare dopo la sincronizzazione della configurazione. Èpossibile tenere traccia dello stato corrente del cluster

		utilizzando questo comando nel dispositivo gestito CLISH: >mostra informazioni cluster
asa_configuration_generation_errors	Distribuzione non riuscita a causa di un errore durante la generazione della configurazione del dispositivo. Se il problema persiste, contattare Cisco TAC.	Dopo aver esaminato i registri USMS sopra menzionati, è possibile verificare quale configurazione causa l'errore. Si tratta in genere di bug in cui è possibile esaminare i log tramite Cisco Bug Tool o contattare Cisco TAC per ulteriori informazioni sulla risoluzione dei problemi.
interface_out_of_date	Distribuzione non riuscita perché le interfacce nel dispositivo non sono aggiornate. Salvare la configurazione nella pagina interfacce e riprovare.	Questo si verifica sui modelli 4100 o 9300 se l'interfaccia non è associata al dispositivo durante o subito prima di un'installazione. Verificare che l'interfaccia

		sia completamente associata o non associata prima di tentare la distribuzione.
errore_pacchetto_periferica	Distribuzione non riuscita a causa di un errore nella generazione della configurazione per il dispositivo. Se il problema persiste, contattare Cisco TAC.	Questo errore indica che non è stato possibile generare la configurazione del dispositivo. Contatta TAC.
timeout_pacchetto_dispositivo	Distribuzione non riuscita a causa di un timeout durante la generazione della configurazione. Se il problema persiste, contattare Cisco TAC.	Questa condizione si può verificare se esiste una latenza tra i dispositivi oltre i limiti normali. Contattare TAC se, dopo la normalizzazione della latenza, il problema persiste.
errori_comunicazione_periferica	Distribuzione non riuscita a causa di un errore di comunicazione con il dispositivo. Verificare la connettività di rete e riprovare la distribuzione.	Questo messaggio è il fallback per qualsiasi problema di comunicazione tra i dispositivi. A causa della sua natura vaga, è scritto come il fallback allo stato che si è verificato un errore di

		connettività sconosciuto.
unable_to_initiate_deployment_dc	Distribuzione non riuscita a causa di un errore durante la distribuzione dei criteri nel dispositivo. Riprovare la distribuzione.	Per risolvere il problema, riprovare. Questo problema può verificarsi quando il FMC non è in grado di avviare la distribuzione a causa di un blocco temporaneo del database.
timeout_errore_dispositivo	Distribuzione al dispositivo non riuscita a causa del timeout. Riprovare la distribuzione.	Questo è relativo alla distribuzione FTD. I processi con FTD attendono 30 minuti per il completamento dell'installazione della spedizione. In caso contrario, scade. In questo caso, verificare la connettività tra i dispositivi e se la connettività è quella prevista, contattare TAC.
errore_dispositivo_download_timeout	Distribuzione non riuscita a causa del	Questo è

	timeout durante il download della configurazione nel dispositivo. Se il problema persiste, contattare Cisco TAC.	relativo alla distribuzione FTD. Impossibile scaricare tutti i file di configurazione e del dispositivo durante la distribuzione a causa di problemi di connettività. Riprovare al termine della verifica della connettività di rete. Se la verifica è stata effettuata, contattare TAC.
configurazione_errore_dispositivo	Distribuzione non riuscita a causa di un errore di configurazione. Se il problema persiste, contattare Cisco TAC.	Eventuali errori nella configurazione generata da FMC per il dispositivo dovrebbero generare questo errore dopo l'applicazione. Ènecessario analizzarli nei log USMS per verificare quali problemi vengono rilevati e tentare di ripristinarli. Dopo aver riparato il bug, in genere è necessario l'intervento di TAC e la creazione di bug se sui log

		non è possibile trovare una corrispondenza con un difetto noto di Cisco Bug Search Tool.
deployment_timeout_no_response_from_device	Distribuzione non riuscita a causa di un timeout durante la comunicazione con il dispositivo. Se il problema persiste, contattare Cisco TAC.	Questo timeout si verifica se il FMC non ha ricevuto risposta da un dispositivo dopo 45 minuti o prima, a seconda della versione. Errore di comunicazione. Verificare la comunicazione e, se verificato, contattare TAC.
errore_dispositivo_modifica_master	Distribuzione al cluster non riuscita. L'unità master è stata modificata. Riprovare la distribuzione.	Per una distribuzione di installazione cluster FTD, questo errore viene indicato se il nodo master cambia quando è in corso la distribuzione nel dispositivo (post-

		notifica). Riprovare quando il nodo master è stabile. Èpossibile tenere traccia dello stato corrente dei membri del cluster utilizzando questo comando nel dispositivo gestito CLISH: >mostra informazioni cluster
errore_dispositivo_master_sconosciuto	Distribuzione al cluster non riuscita a causa di un errore nell'identificazione dell'unità master. Riprovare la distribuzione.	Impossibile determinare il nodo master corrente durante la distribuzione. Ciò potrebbe essere dovuto in genere a un paio di possibilità: Problemi di connettività oppure impossibile aggiungere il master corrente al cluster in FMC. Il problema dovrebbe essere risolto dopo il ripristino della connettività o dopo l'aggiunta del master corrente al cluster FMC e il tentativo

		verrà ripetuto. Èpossibile tenere traccia dello stato corrente del cluster utilizzando questo comando nel dispositivo gestito CLISH: >mostra informazioni cluster
cd_deploy_app_sync	Distribuzione non riuscita perché è in corso la sincronizzazione della configurazione del cluster. Riprovare la distribuzione.	Questo problema può verificarsi se il dispositivo è in App Sync. Al termine di App Sync, riprovare a eseguire la distribuzione.
distribuzione_cd_esistente	Distribuzione non riuscita a causa di un conflitto con la distribuzione precedente in corso. Se il problema persiste, contattare Cisco TAC.	Ciò può verificarsi se una distribuzione è ancora in corso da un lato, ma non dall'altro. Queste cause sono in genere causate da problemi di comunicazione tra i dispositivi. Contattare TAC se, dopo il timeout, non è ancora possibile eseguire la distribuzione.

Contatta TAC per assistenza

Nel caso in cui le informazioni sopra riportate non consentano la distribuzione di una policy o se il problema non sembra essere relativo a un comportamento documentato pre-esistente, eseguire la procedura descritta nel collegamento successivo per generare un file per la risoluzione dei problemi e contattare TAC per l'analisi e la creazione di bug.

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html