Logboekregistratie configureren op FTD via FMC

Inhoud

Inleiding

In dit document wordt de logconfiguratie beschreven voor een FirePOWER Threat Defense (FTD) via Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FirePOWER-technologie
- Basiskennis van de adaptieve security applicatie (ASA)
- Syslog-protocol

Gebruikte componenten

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

- ASA Firepower Threat Defense Image voor ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) die softwareversie 6.0.1 en hoger uitvoert
- ASA Firepower Threat Defense Image voor ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA

5555-X, ASA 5585-X) die software versie 6.0.1 en hoger heeft
- FMC, versie 6.0.1 en hoger

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

Achtergrondinformatie

De FTD-systeemlogbestanden bieden u de informatie om het FTD-apparaat te controleren en problemen op te lossen. De logbestanden zijn zowel nuttig bij routinematige probleemoplossing als bij de verwerking van incidenten. Het FTD-apparaat ondersteunt zowel lokale als externe houtkap.

Local logging kan u helpen bij het oplossen van de actieve problemen. Externe houtkap is een methode voor het verzamelen van logbestanden van het FTD-apparaat naar een externe Syslogserver. Vastlegging op een centrale server helpt bij het verzamelen van logbestanden en waarschuwingen. Externe houtkap kan u helpen bij het correleren van de log en het verwerken van incidenten.

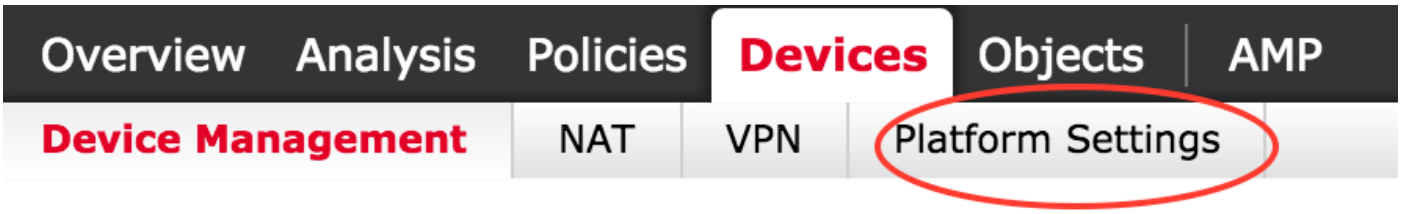
Voor lokale houtkap ondersteunt het FTD-apparaat console, interne bufferoptie en de vastlegging van de Secure Shell (SSH)-sessie.

Voor externe vastlegging ondersteunt het FTD-apparaat de externe Syrische server en de e-mailRelay server.

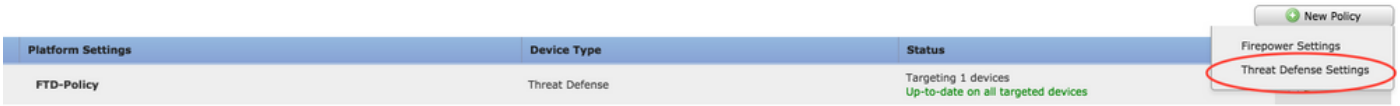
> **Opmerking:** Let bij een groot verkeersvolume door het apparaat op het type houtkap/ernst/snelheidsbeperking. Doe dit om het aantal logbestanden te beperken, zodat u geen invloed hebt op de firewall.

Configureren

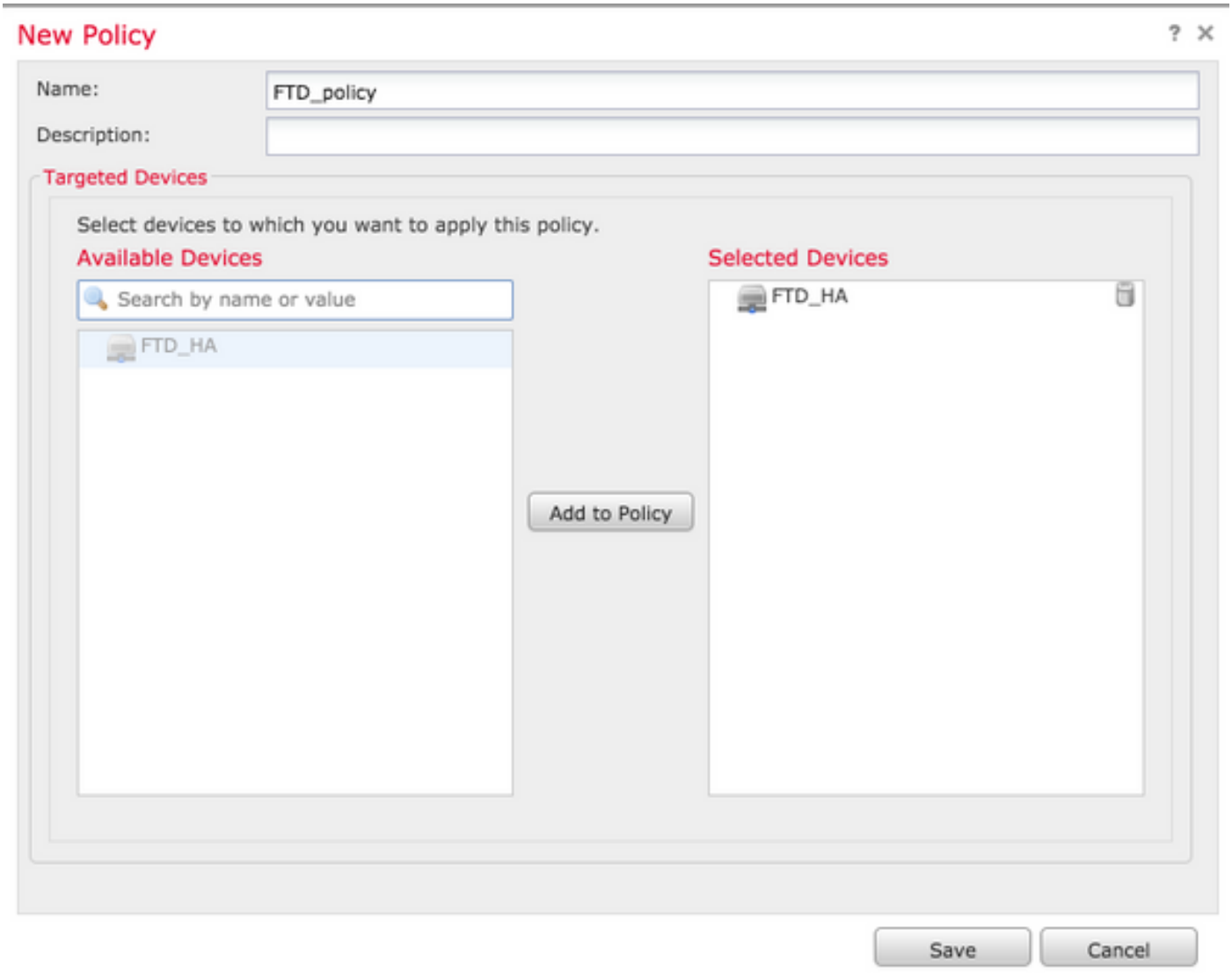
Alle met houtkap verband houdende configuraties kunnen worden geconfigureerd wanneer u naar het scherm navigeert Platform Settings tabblad onder het kopje Devices tab. Kies Devices > Platform Settings zoals in deze afbeelding wordt weergegeven.



Klik op het pictogram potlood om het bestaande beleid te bewerken of klik op **New Policy**en kies vervolgens **Threat Defense Settings**om een nieuw FTD-beleid te creëren zoals in deze afbeelding wordt getoond.



Kies het FTD-apparaat om dit beleid toe te passen en klik **Save** zoals in deze afbeelding wordt weergegeven.



Configuratie Global SLOG configureren

Er zijn bepaalde configuraties die van toepassing zijn op zowel lokale als externe houtkap. In dit gedeelte worden de verplichte en optionele parameters besproken die voor Syslog kunnen worden ingesteld.

Instellen vastlegging

Vastlegging zijn opties voor lokale en externe vastlegging van toepassing. Kies om de instelling voor vastlegging te configureren **Devices > Platform Settings**.

Kies **Syslog > Logging Setup**.

Basisloginstellingen

- Enable Logging: Controleer het **Enable Logging** Schakel dit vakje in om houtkap mogelijk te maken. Dit is een verplichte optie.
- Enable Logging on the failover standby unit: Controleer het **Enable Logging on the failover standby unit** aanvinkvakje om houtkap te configureren op de standby-FTD die deel uitmaakt van een FTD High Availability cluster.
- Send syslogs in EMBLEM format: Controleer het **Send syslogs in EMBLEM format** Schakel dit vakje in om het formaat van SSIG als EMBLEM voor elke bestemming in te schakelen. Het EMBLEM-formaat wordt voornamelijk gebruikt voor de CiscoWorks Resource Manager Essentials (RME) SYL-analyzer. Dit formaat komt overeen met het Cisco IOS-softwarerelease dat door de routers en de switches is geproduceerd. Het is alleen beschikbaar voor UDP Syslog-servers.
- Send debug messages as syslogs: Controleer het **Send debug messages as syslogs** Schakel dit vakje in om de debug-logbestanden als slogberichten naar de Syslog-server te verzenden.
- Memory size of the Internal Buffer: Geef de interne geheugenbuffergrootte op waar FTD de loggegevens kan opslaan. De loggegevens worden gedraaid als de bufferlimiet wordt bereikt.

FTP-serverinformatie (optioneel)

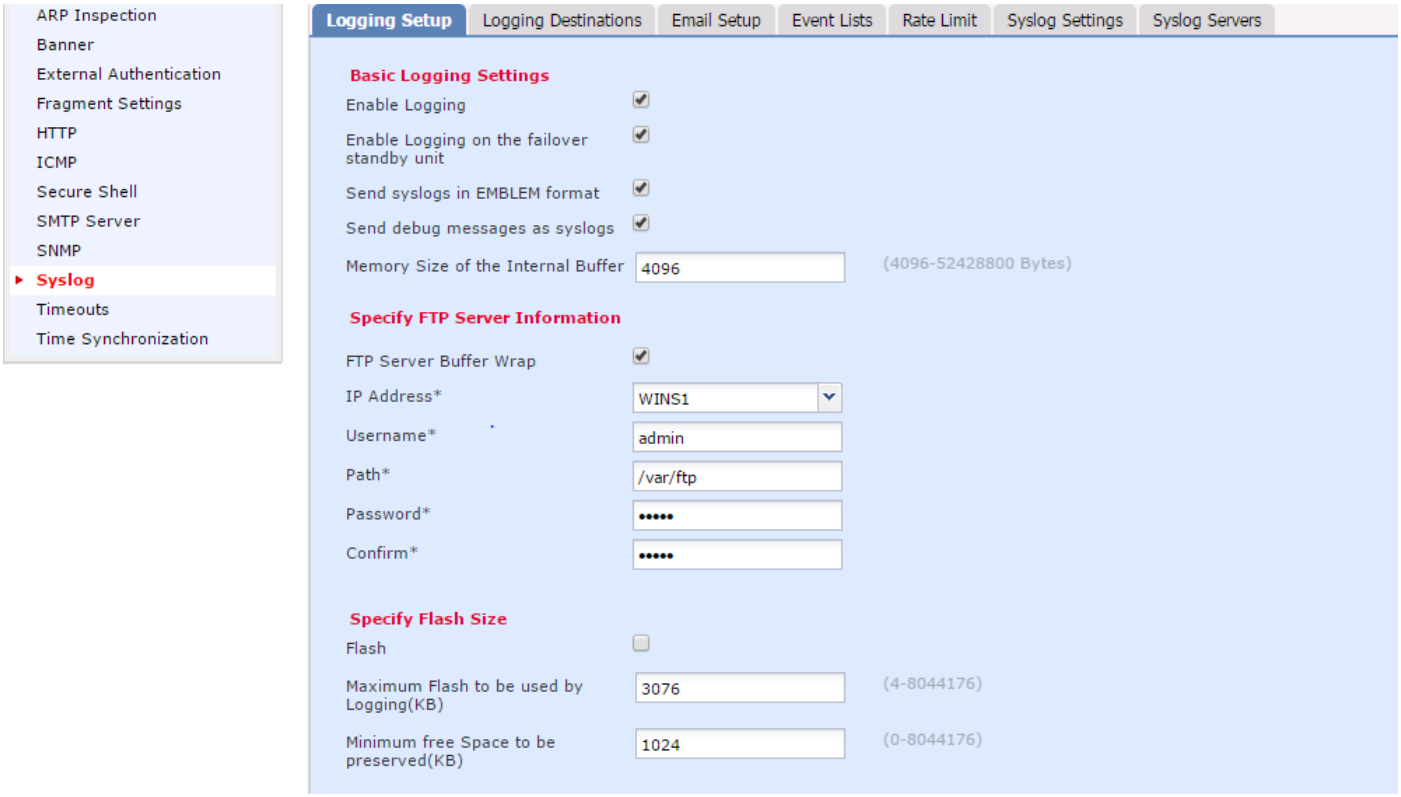
Specificeer FTP-servergegevens als u de loggegevens naar FTP-server wilt verzenden voordat de interne buffer wordt overschreven.

- FTP Server Buffer Wrap: Controleer het **FTP Server Buffer Wrap** Schakel dit vakje in om de gegevens van het bufferlogbestand naar de FTP-server te sturen.
- IP Address: Voer het IP-adres van de FTP-server in.
- Username: Voer de gebruikersnaam van de FTP-server in.
- Path: Voer het directory pad van de FTP server in.
- Password: Voer het wachtwoord van de FTP-server in.
- Confirm: Voer hetzelfde wachtwoord nogmaals in.

Flitsformaat (optioneel)

Specificeer de flitsgrootte als u de loggegevens wilt opslaan om flitser te maken wanneer de interne buffer vol is.

- Flash: Controleer het **Flash** vinkvakje aan om de loggegevens naar de interne flitser te sturen.
- Maximum Flash to be used by Logging(KB): Geef de maximale grootte in KB op van flash-geheugen dat kan worden gebruikt voor houtkap.
- Minimum free Space to be preserved(KB): Geef de minimumgrootte op in KB van het flitsgeheugen dat moet worden bewaard.



Klik **Save** om de platforminstelling op te slaan. Kies het **Deploy** Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Lijst van gebeurtenissen

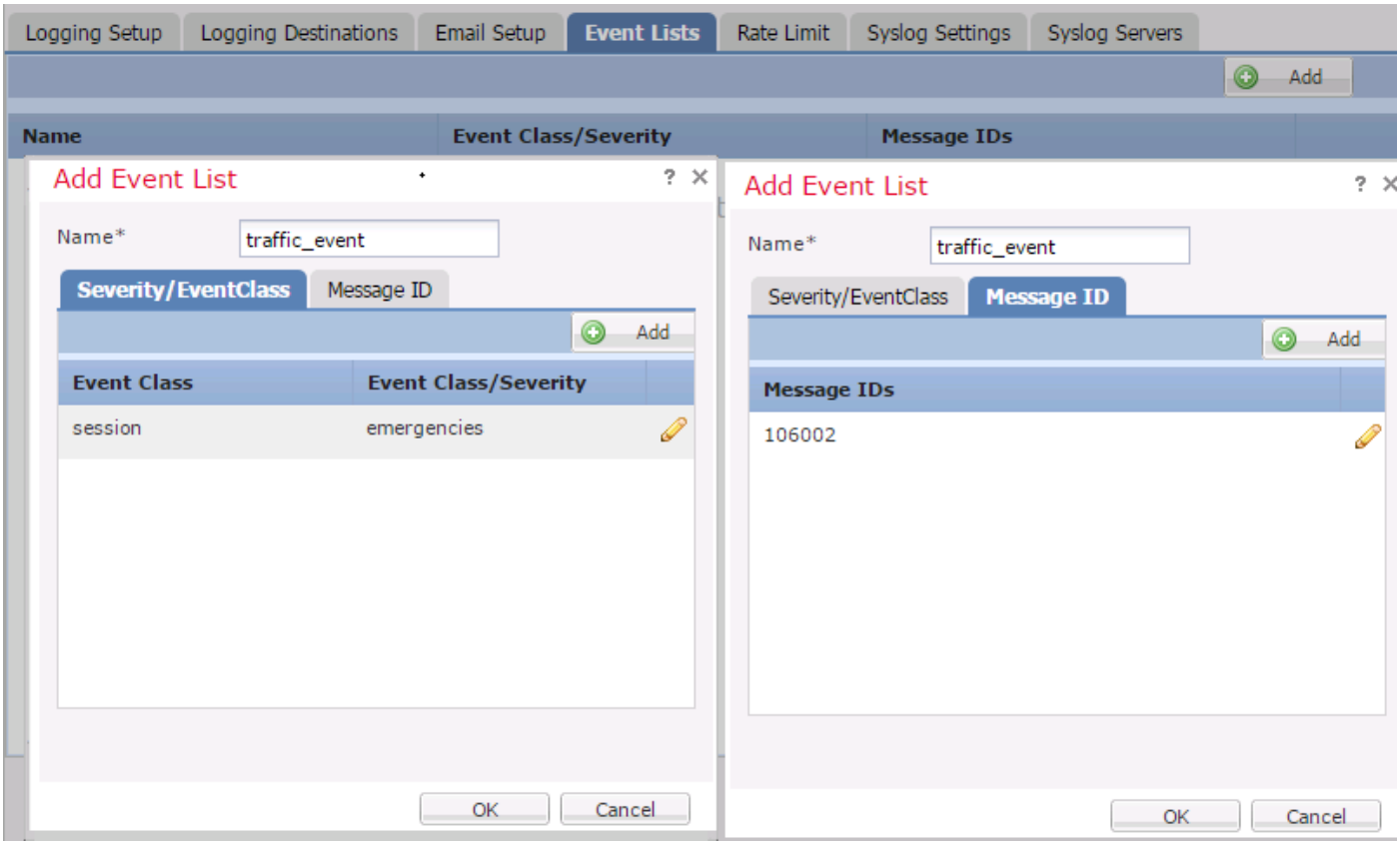
Met de optie Lijst van gebeurtenissen configureren kunt u een lijst van gebeurtenissen maken/bewerken en specificeren welke loggegevens u in het filter van de lijst van gebeurtenissen wilt opnemen. De lijst van gebeurtenissen kan worden gebruikt wanneer u Logging Filters onder Logging bestemmingen configureren.

Het systeem staat twee opties toe om de functionaliteit van lijsten van aangepaste gebeurtenissen te gebruiken.

- Klasse en ernst
- Bericht ID

Om de lijsten van aangepaste gebeurtenissen te configureren kiest u **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** en klik **Add**. Dit zijn de opties:

- Name: Voer de naam van de eventlijst in.
- Severity/Event Class: Klik in het gedeelte Severo/Event Class op **Add**.
- Event Class: Kies de gebeurtenis class in de vervolgkeuzelijst voor het gewenste type loggegevens. Een Event Class definieert een reeks SLOG-regels die dezelfde functies weergeven. Er is bijvoorbeeld een Event Class voor de sessie die alle Syslogs bevat die betrekking hebben op de sessie.
- Syslog Severity: Kies de ernst in de vervolgkeuzelijst voor de gekozen Event Class. De ernst kan variëren van 0 (noodgeval) tot 7 (het zuiveren).
- Message ID: Als u geïnteresseerd bent in specifieke loggegevens met betrekking tot een bericht-ID, klikt u op **Add** Zo plaatst u een filter op basis van de bericht-ID.
- Message IDs: Specificeer het bericht-ID als individueel/bereikformaat.



Klik **OK** om de configuratie op te slaan.

Klik **Save** om de platforminstelling op te slaan. Selecteer **Deploy**Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy**om de invoering van de platforminstelling te starten.

Snelheidsbeperking

De optie Snelheidslimiet definieert het aantal berichten dat naar alle geconfigureerde bestemmingen kan worden verzonden en definieert de ernst van het bericht waaraan u tarieflimieten wilt toewijzen.

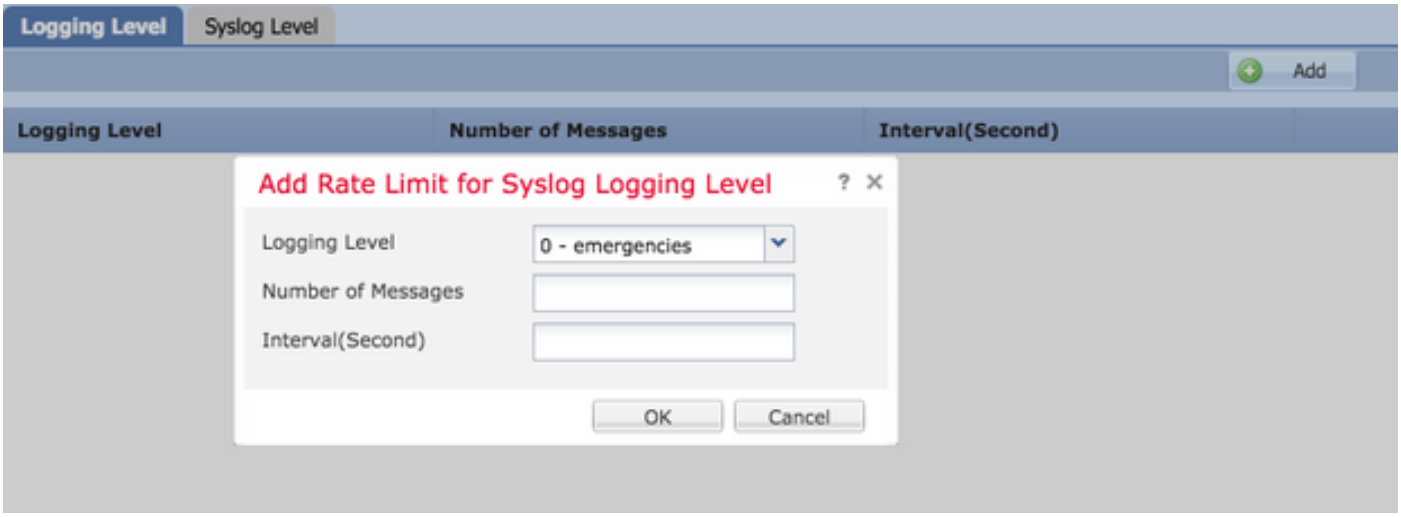
Om de lijsten van aangepaste gebeurtenissen te configureren kiest u **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. U hebt twee opties op basis waarvan u de snelheidsbeperking kunt instellen:

- Vastleggingsniveau
- Syslogniveaus

Om de op houtkap gebaseerde snelheidsbeperking in te schakelen, kiest u **Logging Level** en klik **Add**.

- Logging Level: Van de **Logging Level** Selecteer het logniveau waarvoor u de snelheidsbeperking wilt uitvoeren.
- Number of Messages: Geef het maximale aantal Syslog-berichten op dat binnen het opgegeven interval moet worden ontvangen.
- Interval(Second): Gebaseerd op het parameter Aantal eerder gevormde berichten, voer het tijdsinterval in waarin een vaste reeks van Syslog berichten kan worden ontvangen.

Het aantal Syslog is het aantal berichten/intervallen.

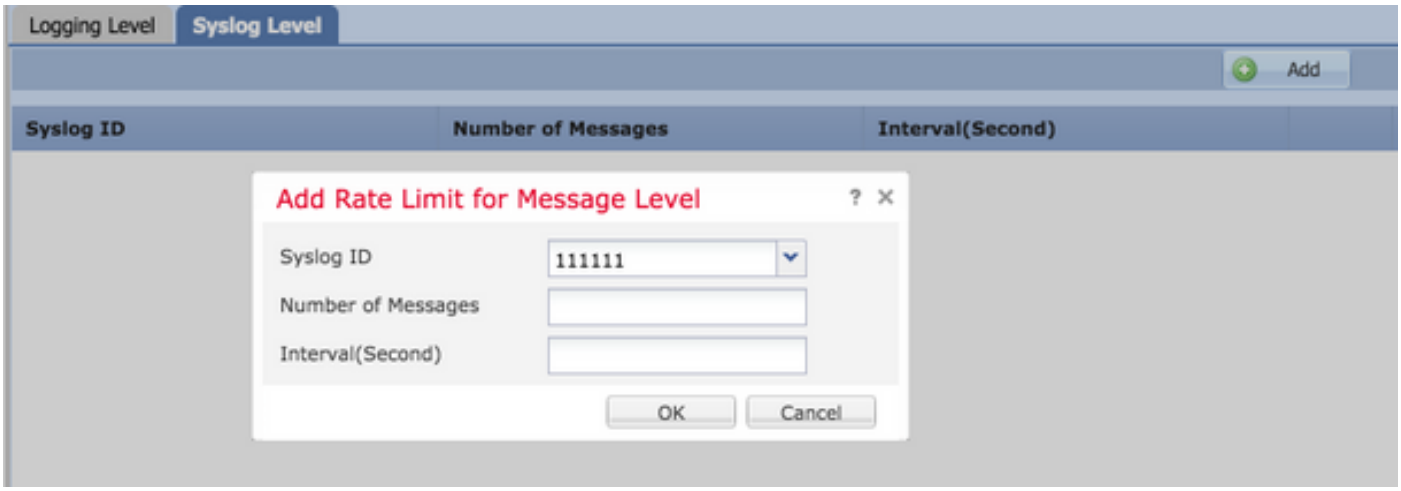


Klik **OK** om de configuratie van het logniveau op te slaan.

Om de op houtkap gebaseerde snelheidsbeperking in te schakelen, kiest u **Logging Level** en klik **Add**.

- Syslog ID: Syslog-ID's worden gebruikt om de Syslog-berichten uniek te identificeren. Van de **Syslog ID** Selecteer de optie ID kopiëren.
- Number of Messages: Geef het maximale aantal syslogberichten op dat binnen het opgegeven interval moet worden ontvangen.
- Interval(Second): Gebaseerd op het parameter Aantal eerder gevormde berichten, voer het tijdsinterval in waarin een vaste reeks van Syslog berichten kan worden ontvangen.

Het snelheidscijfer van Syslog is het aantal berichten/interfaces.



Klik **OK** om de configuratie op het niveau van de snelkoppeling op te slaan.

Klik **Save** om de platforminstelling op te slaan. Selecteer **Deploy**Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

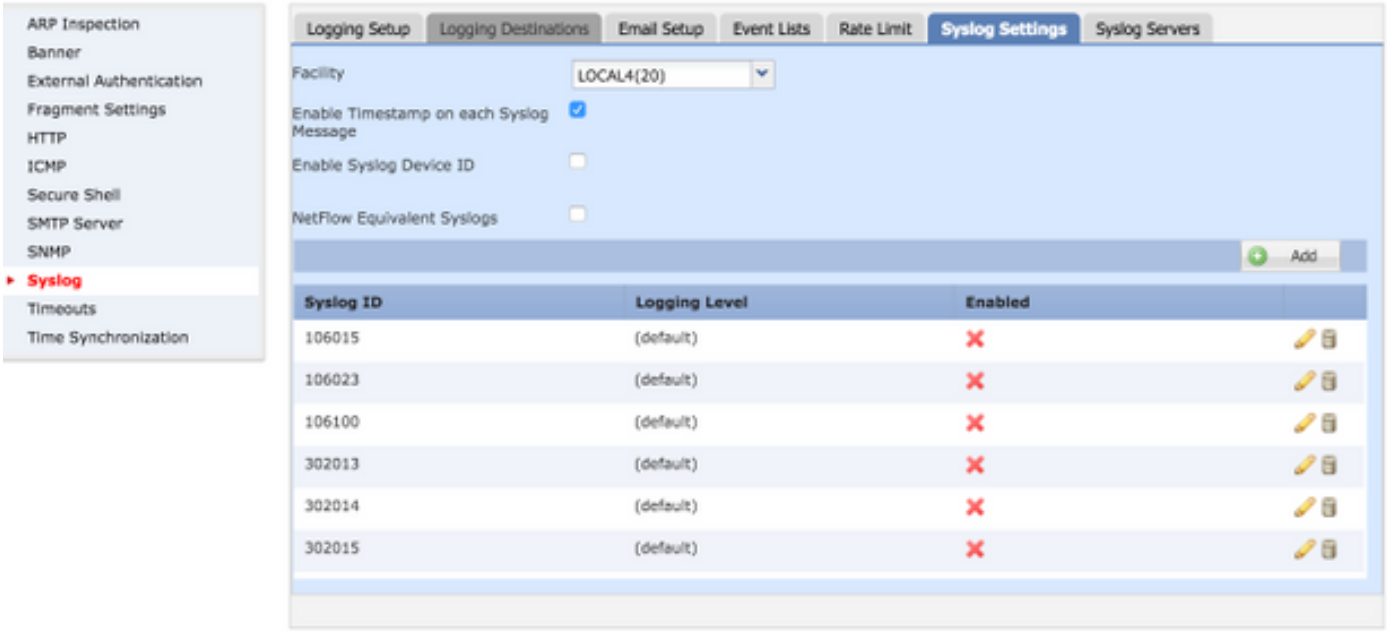
Instellingen begrijpen

De instellingen van het systeem maken het mogelijk de waarden van de faciliteit in de Syslog berichten te specificeren. U kunt de timestamp ook in logberichten en andere Syslog server-specifieke parameters toevoegen.

Om de lijsten van aangepaste gebeurtenissen te configureren kiest u **Device > Platform Setting > Threat**

Defense Policy > Syslog > Syslog Settings.

- Facility: Er wordt een installatiecode gebruikt om het type programma te specificeren dat het bericht registreert. Berichten met verschillende faciliteiten kunnen anders worden behandeld. Van de **Facility** kies de waarde van de faciliteit.
- Enable Timestamp on each Syslog Message: Controleer het **Enable Timestamp on each Syslog Message** aanvinkvakje om de tijdstempel in de Syslog-berichten op te nemen.
- Enable Syslog Device ID: Controleer het **Enable Syslog Device ID** Schakel dit vakje in om een id van een apparaat in de Syslog-berichten die geen EMBLEM-formaat hebben.
- Netflow Equivalent Syslogs: Controleer het **Netflow Equivalent Syslogs** Schakel dit vakje in om NetFlow-equivalente systemen te verzenden. Dit kan de prestaties van het apparaat beïnvloeden.
- Geef een specifieke snelkoppeling-id op: Klik op om de extra software-id te specificeren **Add** en de **Syslog ID/ Logging Level** aanvinkvakje.



Klik **Save** om de platforminstelling op te slaan. Selecteer **Deploy**Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Lokale vastlegging configureren

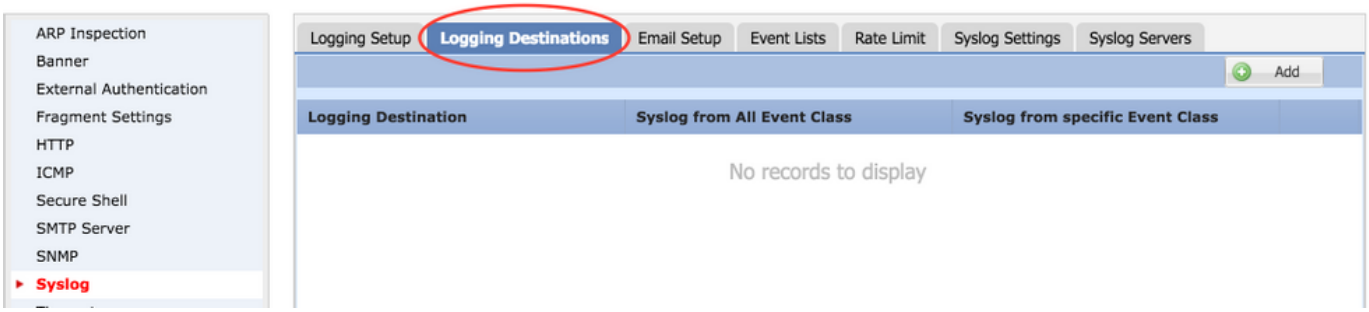
Het vak Logging Destination kan worden gebruikt om de houtkap op specifieke bestemmingen te configureren.

De beschikbare interne houtkapbestemmingen zijn:

- Interne buffer: Logt aan de interne houtkapbuffer (houtkap gebufferd)
- console: Zendt logs naar de console (houtkapconsole)
- SSH-sessies: Logs Sjol naar SSH-sessies (terminalmonitor)

Er zijn drie stappen om lokale vastlegging te configureren.

Stap 1. Kies **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.



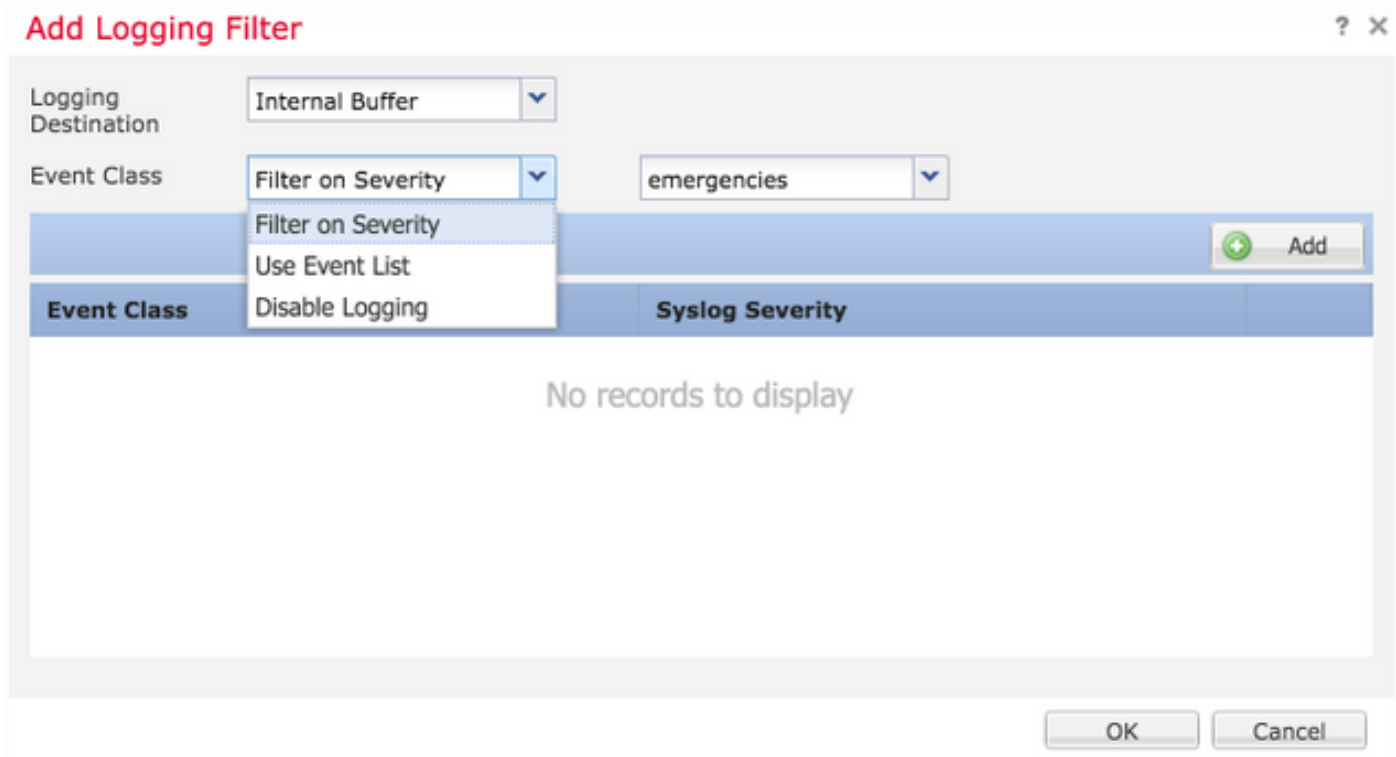
Stap 2. Klik op **Add** om een vastlegging filter voor een specifiek gebied toe te voegen **logging destination.**

Logbestemming: Kies de gewenste logbestemming in het **Logging Destination** vervolgkeuzelijst als interne buffer, console of SSH-sessies.

Event class: Van de **Event Class** Selecteer een Event class. Zoals eerder beschreven zijn de Event Classes een reeks Syslogs die dezelfde functies weergeven. De Event class kan op de volgende manieren worden geselecteerd:

- Filter on Severity: Event Klasse filter op basis van de ernst van de symbolen.
- User Event List: De beheerders kunnen de specifieke (eerder beschreven) lijst van gebeurtenis met hun eigen klassen van douanegebeurtenissen maken en hen in deze sectie verwijzen.
- Disable Logging: Gebruik deze optie om houtkap voor het gekozen logdoelniveau en vastlegging uit te schakelen.

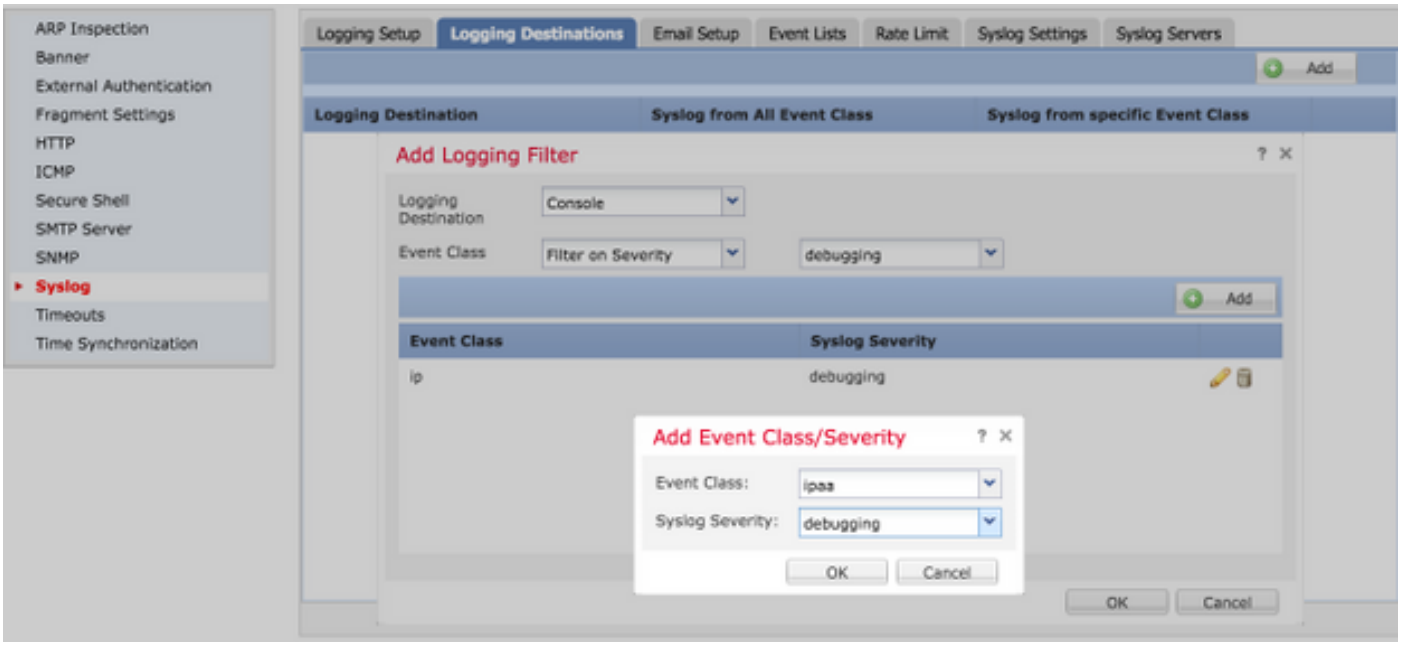
Logniveau: Kies het logniveau in de vervolgkeuzelijst. Het bereik van het houtkapniveau varieert van 0 (noodgevallen) tot 7 (het fouilleren).



Stap 3. Klik om een afzonderlijke Event-klasse aan dit Logging filter toe te voegen **Add**.

Event Class: Kies de Event Class van het **Event Class** (Functie).

Syslog Severity: Kies de ernst van het systeem **Syslog Severity** (Functie).



Klik **OK** nadat het filter is geconfigureerd om het filter toe te voegen voor een specifieke logbestemming.

Klik **Save** om de platforminstelling op te slaan. Kies **Deploy**Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy** om de installatie van het platform te starten.

De externe vastlegging configureren

Kies om externe vastlegging te configureren **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

FTD ondersteunt dit soort externe houtkap.

- Syrische server: Logbestanden worden naar de afstandsbediening verzonden.
- SNMP-trap: Zendt de logs uit als een SNMP-val.
- E-mail: De logbestanden worden per e-mail verzonden met een vooraf ingestelde mailrelais server.

De configuratie voor de externe vastlegging en de interne vastlegging zijn hetzelfde. De selectie van de bloggende bestemmingen bepaalt het type houtkap dat wordt geïmplementeerd. Het is mogelijk om Event Classes te configureren op basis van Aangepaste Event List naar de afstandsserver.

Remote-bladeserver

Syslog-servers kunnen worden ingesteld om logbestanden op afstand vanaf de FTD te analyseren en op te slaan.

Er zijn drie stappen om de afstandsbediening van Syslog-servers te configureren.

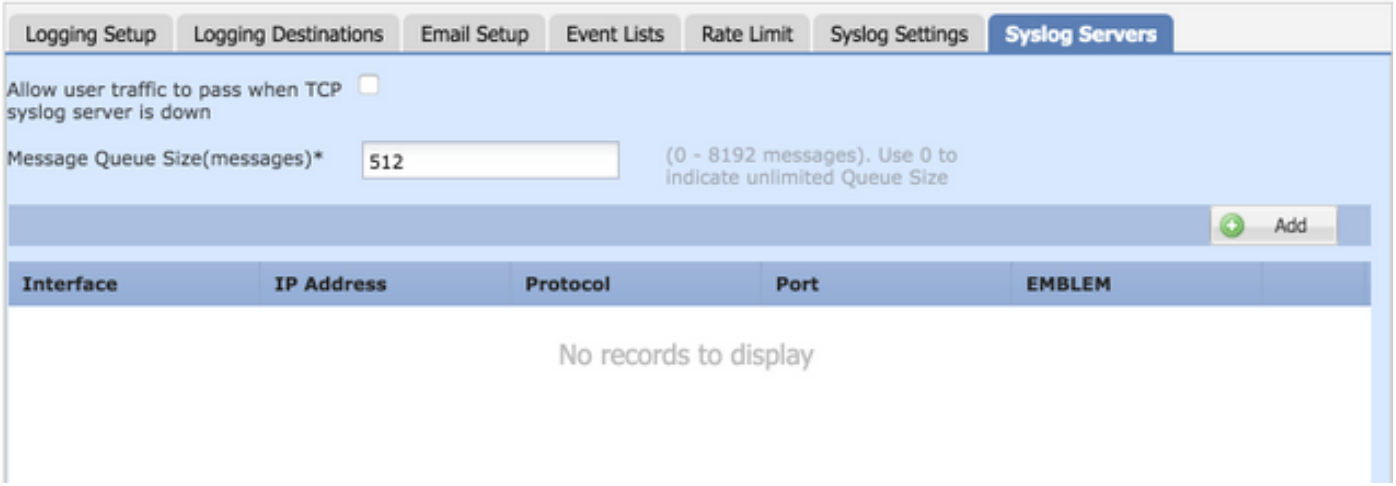
Stap 1. Kies **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**.

Stap 2. Configureer de parameter die gerelateerd is aan de Syrische server.

- Toestaan gebruikersverkeer om over te gaan wanneer TCP syslg server is: Als een TCP

Syslog server in het netwerk is opgesteld en niet bereikbaar is, wordt het netwerkverkeer door de ASA ontkend. Dit is alleen van toepassing wanneer het transportprotocol tussen de ASA en de Syslog server TCP is. Controleer het **Allow user traffic to pass when TCP syslog server is down** Schakel dit vakje in om verkeer door de interface te laten passeren wanneer de systeemserver is uitgeschakeld.

- Grootte van berichtenwachtrij: De grootte van de berichtwachtrij is het aantal berichten dat in de FTD in de wachtrij staat wanneer de afstandsbediening van de sneltoetsen bezig is en geen logberichten accepteert. De standaardinstelling is 512 berichten en het minimum is 1 bericht. Als 0 in deze optie wordt gespecificeerd, wordt de rijgrootte als onbeperkt beschouwd.



Stap 3. Klik op om externe systeemservers toe te voegen **Add**.

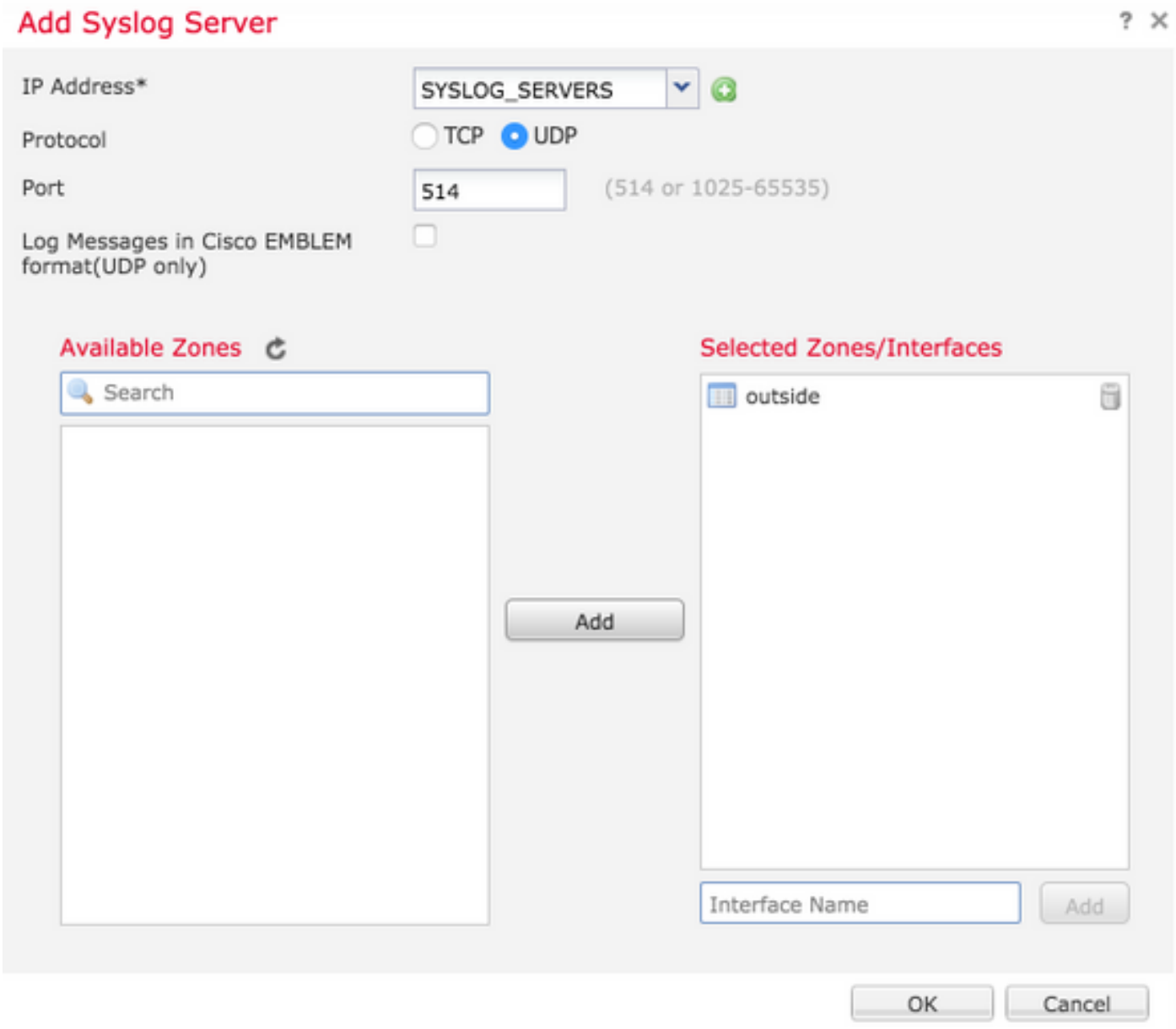
IP Address: Van de **IP Address** Selecteer een netwerkobject met de systeemservers in de lijst. Als u geen netwerkobject hebt gemaakt, klikt u op het pictogram plus (+) om een nieuw object te maken.

Protocol: Klik op of **TCP** of **UDP** radioknop voor de Syslog-communicatie.

Port: Voer het havennummer van de Syslog-server in. Standaard is het 514.

Log Messages in Cisco EMBLEM format(UDP only): Klik op het **Log Messages in Cisco EMBLEM format (UDP only)** Schakel dit vakje in om deze optie in te schakelen als er berichten in de Cisco EMBLEM-indeling moeten worden geregistreerd. Dit is alleen van toepassing op USDP-gebaseerde Syslog.

Available Zones: Voer de beveiligingszones in waarover de syslogserver bereikbaar is en verplaats deze naar de kolom Geselecteerde gebieden/interfaces.



Klik **OK** en **Save** om de configuratie op te slaan.

Klik **Save** om de platforminstelling op te slaan. Kies **Deploy**Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

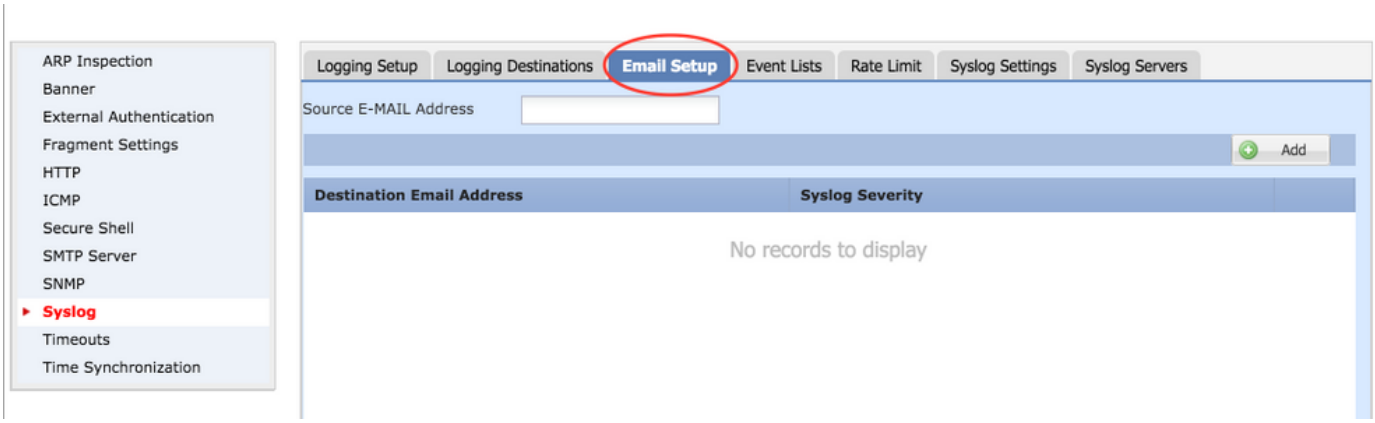
E-mailinstelling voor vastlegging

FTD stelt u in staat om het formulier naar een specifiek e-mailadres te versturen. E-mail kan alleen als houtkapbestemming worden gebruikt als er al een e-mailrelaisserver is ingesteld.

Er zijn twee stappen om e-mailinstellingen voor de Syslogs te configureren.

Stap 1. Kies **Device > Platform Setting > Threat Defense Policy > Syslog >Email Setup**.

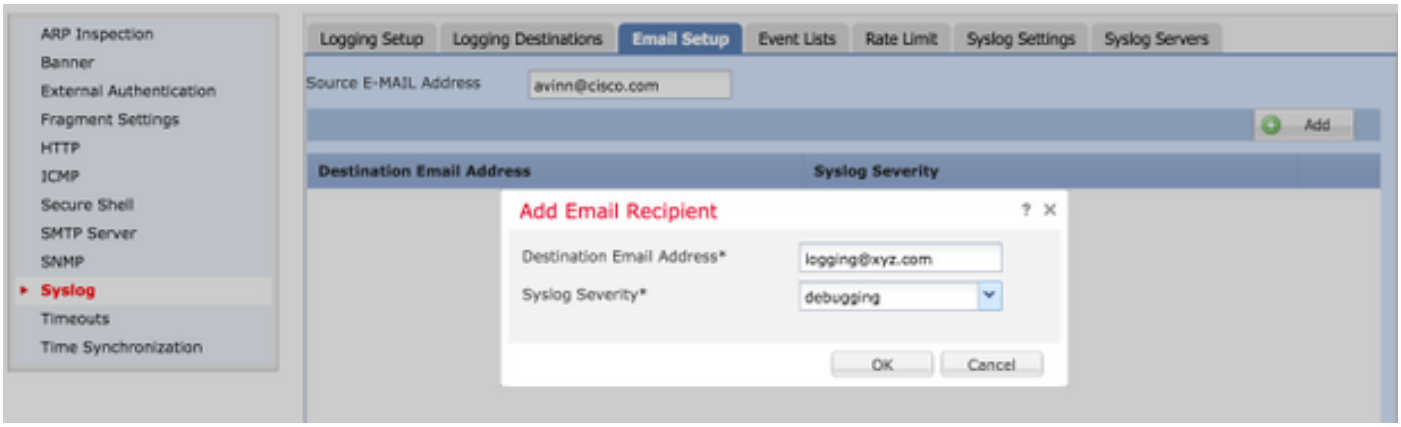
Source E-MAIL Address: Voer het bron-e-mailadres in dat in alle e-mails die vanuit de FTD worden verstuurd en die de Syslogs bevatten.



Stap 2. Klik om het doeladres en de ernst van het bericht te configureren op **Add**.

Destination Email Address: Voer het bestemming e-mailadres in waar de slogberichten worden verzonden.

Syslog Severity: Kies de ernst van het systeem **Syslog Severity** (Functie).



Klik **OK** om de configuratie op te slaan.

Klik **Save** om de platforminstelling op te slaan. Kies **Deploy**Selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

- Controleer de FTD Syslog-configuratie in de FTD CLI. Meld u aan bij de beheerinterface van de FTD en voer het volgende in **system support diagnostic-cli** Opdracht om in de diagnostische CLI te troosten.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

- Verzeker u ervan dat de Syslog server bereikbaar is vanaf de FTD. Meld u aan bij de FTD Management Interface via SSH en controleer de connectiviteit met de **ping** uit.

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

- U kunt een pakketvastlegging nemen om de connectiviteit tussen de FTD en de Syrische server te verifiëren. Meld u aan bij de FTD Management Interface via SSH en voer de opdracht in **system support diagnostic-cli**. Raadpleeg voor de opdrachten pakketvastlegging ASA Packet Captures met CLI en ASDM Configuratievoorbeeld.
- Zorg ervoor dat de beleidsuitvoering met succes wordt toegepast.

Gerelateerde informatie

- Cisco Firepower Threat Defense Quick Start Guide voor de ASA
- Technische ondersteuning en documentatie – Cisco Systems