Syslog-applicatie (ASA) voor adaptieve security applicatie configureren

Inhoud

Inleiding Achtergrondinformatie Voorwaarden Vereisten Gebruikte componenten Basic-netwerkmodule Logboekgegevens naar de interne buffer sturen Logboekgegevens naar een syslogserver verzenden Logboekgegevens als e-mailberichten verzenden Logboekgegevens naar de seriële console sturen Logboekgegevens verzenden naar een Telnet/SSH-sessie Logberichten weergeven op de ASDM Logbestanden verzenden naar een SNMP-beheerstation Tijdstempels aan systeemlogs toevoegen Voorbeeld 1 Syslog voor basisconfiguratie configureren met ASDM Verzend Syslog-berichten via VPN naar een Syslog-server Configuratie centrale ASA ASA-configuratie op afstand Geavanceerde systeemsleuf Gebruik de Berichtenlijst Voorbeeld 2 **ASDM-configuratie** De berichtklasse gebruiken Voorbeeld 3 **ASDM-configuratie** Verzend debug log berichten naar een syslog server Gebruik van de Lijst van het Vastleggen en Berichtklassen samen ACL-treffers in logbestanden Syslog-generatie blokkeren op een standby ASA Verifiëren Problemen oplossen %ASA-3-201008: nieuwe verbindingen verbieden Oplossing Gerelateerde informatie

Inleiding

Dit document beschrijft voorbeeldconfiguratie die aantoont hoe u verschillende registratieopties kunt configureren op ASA waarbij code versie 8.4 of hoger wordt uitgevoerd.

Achtergrondinformatie

ASA versie 8.4 heeft zeer korrelige filtertechnieken geïntroduceerd om slechts bepaalde gespecificeerde

syslog-berichten te kunnen presenteren. In het gedeelte Basic Syslog van dit document wordt een traditionele syslog-configuratie getoond. Het gedeelte Advanced Syslog van dit document toont de nieuwe syslog-functies in Versie 8.4. Raadpleeg de <u>Cisco Security Appliance System Log Messages Guides</u> voor de volledige handleiding voor logberichten van het systeem.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- ASA 5515 met ASA softwareversie 8.4
- Cisco Adaptive Security Device Manager (ASDM), versie 7.1.6

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.

Opmerking: Raadpleeg <u>ASA 8.2</u>: <u>Syslog configureren met ASDM</u> voor meer informatie over vergelijkbare configuratiedetails met ASDM versie 7.1 en hoger.</u>

Basic-netwerkmodule

Voer deze opdrachten in om vastlegging, logbestanden en configuratie-instellingen voor weergave in te schakelen.

- **logboekregistratie inschakelen** Schakelt de transmissie van syslogberichten naar alle uitvoerlocaties in.
- no logging enabled Schakelt loggen uit voor alle uitvoerlocaties.
- **logboekregistratie tonen** Toont de inhoud van de syslogbuffer en informatie en statistieken die betrekking hebben op de huidige configuratie.

ASA kan syslog berichten naar diverse bestemmingen verzenden. Voer de opdrachten in deze secties in om de locaties te specificeren waarvan u wilt dat de sysloginformatie wordt verzonden:

Logboekgegevens naar de interne buffer sturen

<#root>
logging buffered
severity_level

Externe software of hardware is niet vereist wanneer u de syslogberichten in de interne ASA-buffer opslaat. Voer de opdracht **logboekregistratie tonen in** om de opgeslagen syslog-berichten te bekijken. De interne buffer heeft een maximumgrootte van 1 MB (configureerbaar met het bevel van de **logboekbuffer-grootte**). Als gevolg daarvan kan het heel snel worden verpakt. Houd dit in gedachten wanneer u een registratieniveau voor de interne buffer kiest aangezien meer breedsprakige niveaus van registreren snel kunnen vullen en verpakken, de interne buffer.

Logboekgegevens naar een syslogserver verzenden

<#root>				
logging host				
<pre>interface_name ip_address</pre>	[tcp[/port]	<pre> udp[/port]]</pre>	[format	emblem]
logging trap				
severity_level				
logging facility				
number				

Een server die een syslogtoepassing in werking stelt wordt vereist om syslogberichten naar een externe gastheer te verzenden. ASA verzendt standaard syslog op UDP-poort 514, maar protocol en poort kunnen worden gekozen. Als TCP is gekozen als het logprotocol, dan zorgt dit ervoor dat ASA syslogs via een TCP verbinding naar de syslog server stuurt. Als de server ontoegankelijk is of als de TCP-verbinding met de server niet tot stand kan worden gebracht, blokkeert de ASA standaard ALLE nieuwe verbindingen. Dit gedrag kan worden uitgeschakeld als u **logboekregistratie-hostdown** inschakelt. Zie de configuratiegids voor meer informatie over de opdracht **logboekvergunning-hostdown**.

Opmerking: de ASA staat alleen poorten toe die variëren van 1025-65535. Het gebruik van een andere poort resulteert in deze fout: ciscoasa (config)# logboekhost tftp 192.168.1.1 udp/516 WAARSCHUWING: het beveiligingsniveau van de interface Ethernet0/1 is 0. FOUT: Port '516' valt niet binnen het bereik van 1025-65535.

Logboekgegevens als e-mailberichten verzenden

<#root>
logging mail
severity_level
logging recipient-address
email_address
logging from-address
email_address
smtp-server

Een SMTP-server is vereist wanneer u de syslog-berichten in e-mails verstuurt. Correcte configuratie op de SMTP-server is nodig om ervoor te zorgen dat u e-mails van de ASA met succes kunt doorgeven aan de opgegeven e-mailclient. Als dit registratieniveau is ingesteld op een zeer ruim niveau, zoals debug of informatie, kunt u een aanzienlijk aantal syslogs genereren omdat elke e-mail die door deze logconfiguratie wordt verzonden, leidt tot het genereren van vier of meer extra logbestanden.

Logboekgegevens naar de seriële console sturen

<#root>
logging console
severity_level

Met logboekregistratie op console kunnen syslog-berichten op de ASA-console (tty) worden weergegeven wanneer ze zich voordoen. Als de logboekregistratie is geconfigureerd, wordt alle logboekgeneratie op de ASA geratificeerd naar 9800 Gbps, de snelheid van de ASA seriële console. Dit kan ertoe leiden dat syslogs worden gedropt naar alle bestemmingen, die de interne buffer omvatten. Gebruik om deze reden geen logboekregistratie voor overbodige systemen.

Logboekgegevens verzenden naar een Telnet/SSH-sessie

<#root>
logging monitor
severity_level
terminal monitor

De monitor van het registreren laat syslogberichten toe om te tonen aangezien zij voorkomen wanneer u tot de ASA console met Telnet of SSH toegang hebt en de **eind** van het bevel **monitor** wordt uitgevoerd van die zitting. Om het afdrukken van logboeken naar uw sessie te stoppen, voert u de opdracht **terminal geen monitor in**.

Logberichten weergeven op de ASDM

<#root>

logging asdm

severity_level

ASDM heeft ook een buffer die kan worden gebruikt om syslog berichten op te slaan. Voer de opdracht **logboekregistratie** in om de inhoud van de ASDM-syslog-buffer weer te geven.

Logbestanden verzenden naar een SNMP-beheerstation

<#root>
logging history
severity_level
snmp-server host
[if_name] ip_addr
snmp-server location
text
snmp-server contact
text
snmp-server community
key
snmp-server enable traps

Gebruikers hebben een bestaande functionele Simple Network Management Protocol (SNMP)-omgeving nodig om syslog-berichten met SNMP te kunnen verzenden. Zie <u>Opdrachten voor het instellen en beheren</u> <u>van uitvoerbestemmingen</u> voor een volledige verwijzing naar de opdrachten die u kunt gebruiken om uitvoerbestemmingen in te stellen en te beheren. Zie <u>Berichten op prioriteitsniveau</u> voor berichten op prioriteitsniveau.

Tijdstempels aan systeemlogs toevoegen

Om gebeurtenissen te helpen uitlijnen en bestellen, kunnen tijdstempels aan syslogs worden toegevoegd. Dit wordt aanbevolen om problemen op te sporen op basis van tijd. Om tijdstempels in te schakelen, voert u de opdracht **logtijdstempel in**. Hier zijn twee syslog voorbeelden, één zonder de tijdstempel en één met:

%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to identity:172.18.124.136/161 duration 0:02:01 bytes 313 Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes 442 TCP Reset-I

Voorbeeld 1

Deze output toont een steekproefconfiguratie voor het registreren in de **buffer** met het strengheidsniveau van het **zuiveren**.

Dit is voorbeelduitvoer.

%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)

Syslog voor basisconfiguratie configureren met ASDM

Deze procedure demonstreert de ASDM-configuratie voor alle beschikbare syslog-bestemmingen.

 Om het inloggen op de ASA in te schakelen, moet u eerst de fundamentele logparameters configureren. Kies Configuratie > Eigenschappen > Eigenschappen > Vastlegging > Vastlegging. Schakel het selectievakje Logboekregistratie inschakelen in om systemen in te schakelen.



2. Als u een externe server wilt configureren als de bestemming voor syslogs, kiest u **Syslog Servers** in Logging en klikt u op **Add** om een syslog server toe te voegen. Voer in het vak Add Syslog Server de gegevens van de syslog-server in en kies **OK** wanneer u klaar bent.

Cisco ASDM 7.3 for ASA - 10.306.4	4.164					- 0 2
Hone Ra Configuration	ntoring 🗔 Save 📿 Refe	sh 🙆 Badi. 🕥 Forward 🤣 a	edo -		Type topic to rearch	cisco
Fis Yew Losis Wgards Kind Image: State State Image: State State Image: State State Image: State State Image: State State Image: State Image: State Image: State Image: State Image: State Image: State Image: State <t< th=""><th>Internal Construction Specify the number of seal Specify the number of seal Queue See: 512 Alone search for the function of seal Construction of seal Specify the number of seal Queue See: 512</th><th>eh C Back C Forward P Insection of Sectors Sectors Sec Vers. Hole sue logging is enabled in Co IP Address</th><th>eto monta riguration > Device Management > Logging > Loggi Protocol(Port Adid Systog Server Adid Systog Server Adid Systog Server PAddesse: 172.323.1.5 PAddesse: 17</th><th>ng Setup. DHELEM</th><th>Secure</th><th></th></t<>	Internal Construction Specify the number of seal Specify the number of seal Queue See: 512 Alone search for the function of seal Construction of seal Specify the number of seal Queue See: 512	eh C Back C Forward P Insection of Sectors Sectors Sec Vers. Hole sue logging is enabled in Co IP Address	eto monta riguration > Device Management > Logging > Loggi Protocol(Port Adid Systog Server Adid Systog Server Adid Systog Server PAddesse: 172.323.1.5 PAddesse: 17	ng Setup. DHELEM	Secure	
Device Management			Apply	Reset		
				disto	15 🔯 🎉 🛐	5/9/04 10:46:02 AMUTO

3. Kies **E-mail instellen** in vastlegging om syslog-berichten als e-mails naar specifieke ontvangers te verzenden. Specificeer het brone-mailadres in het vakje Bron-e-mailadres en kies **Toevoegen** om het bestemmings-e-mailadres van de e-mailontvangers en de ernst van het bericht te configureren. Klik op **OK** wanneer u klaar bent.

Fix View Tasls Wands Window Help Provide to wards @ Automation @ Attraction @ Attra
🚱 Hone 🖓 Configuration 🔄 Monitoring 📊 Some 🚱 Reflects 🔾 Back 💭 Forward 💡 Help
Device List 07. 9 X Configuration > Device Management > Loging > Lefiel Series
Add 1 Detein JP Connect: Exiter the e-mail address that will be used as the source address when systags are sent as e-mails.
Red G
5 10.105.44.146
Desite Management d1 4
3 System Inage/Configuration
Destination E-Mail Address I administrats con
To copying Setup is
Event Lats severity retrieved for the regions will be the higher of the
Gip Logging Fitters redpents in Canfiguration>Properties=Slogging>Logging
Stado Servers
8 900 mm
Cancel Help
Constant
BT read
G Renate Access WH
G 200-to-300 KW
🚖 Trend Micro Canterit Seourky
Device Management
2 Apply Reset

4. Kies **Apparaatbeheer**, **Vastlegging**, kies **SMTP**, en voer het IP-adres van de primaire server in om het IP-adres van de SMTP-server te specificeren.



5. Als u syslogs als SNMP-traps wilt verzenden, moet u eerst een SNMP-server definiëren. Kies **SNMP** in het menu **Management Access** om het adres van de SNMP-beheerstations en hun specifieke eigenschappen te specificeren.

Cisco ASDM 7.1 for ASA - 10.106.44	166								×
File View Tools Wigards Windo	w Help					Type to	opic to search	60	ale.
🕞 Hore 🦓 Cartiguesian 🛐 Mari	Roring 🔄 Sove 🔇 Refres	th 🔇 Back 🔘 Form	yd 🦻 Helo					CIS	co
Device List d1 P ×	Configuration > Device Me	magement > Managem	and Access > 52012						
Add Delete J Correct Find Go	Configure SHIP parameters	and monogement stations	Intineab						
10.105.44.144	Contact:	edmin	Contract of the second s						
- 5 10.106.44.176 *	ASA Location	office							
Device Management d1 0	Listening Port:	160	Configure Traps						
E Management Access									
ASDM(HTTPS/Teinek/SSH (H. SRI Connect Une (CL))	SNPP Host Access Lat								
E- Pile Access	Interface	IP Address	Community String	SMP Version	(SMP v.3 Ork)	Poli/Trap	UCP Port	+3	
- the DDAD 								E-0	
Management Sension Que								Dele	te
Management Access Rule									
B- St Literaing									
See System Supplementation See State								_	
E Logono +	SWMPv0 USHS								
4 II +	Configure SMPv3 users. Sp	edfy authentication and pr	tvacy options for users according to	the group to which they belong.					
A Device Setup	Group Name	Usernarse	Encrypted Password	Authentication	Encryption A	lgorithm.	AES Size	45	1
Creed.								Edi	t
Citera in the second								Dele	08
Benote Access WW									
Steks-Ste 191									
🚖 Trend Micro Content Security									
Device Management								_	
:				Apply Res	et.				
					disco	15		10,28,06 7:19	00 AMUTC

6. Kies **Toevoegen** om een SNMP-beheerstation toe te voegen. Voer de SNMP-hostgegevens in en klik op **OK**.

🔁 Add SNMP Hos	t Access Entry
Interface Name:	inside 🗸
IP Address:	172.22.1.5
UDP Port:	162
Community String:	••••
SNMP Version:	2c 🗸 🗸
Server Poll/Trap Sp Select a specified Poll V Trap	ecification ————————————————————————————————————
ОК	Cancel Help

7. Kies **Logfilters** in de logsectie om logbestanden naar een van de eerder genoemde bestemmingen te kunnen versturen. Dit presenteert u met elke mogelijke logboekbestemming en het huidige niveau van logboeken die naar die bestemmingen worden verzonden. Kies de gewenste bestemming voor vastlegging en klik op **Bewerken**. In dit voorbeeld wordt de bestemming 'Syslog Servers' gewijzigd.

Cisco ASDM 7.1 for ASA - 10.106.44	164					
File View Tools Wizards Winds	w Help				Pype topic to search	🚳 alatha
🕞 Hore 🦓 Cantauration 🔯 Mon	Rong 🔚 Sove 🔇 Refresh 🔇 Da	ich. 🜔 Forward 🧳 Help				CISCO
Device List d* P ×	Configuration > Device Management	L> Logging > Logging filters				
🗣 Add 🁔 Delete 🖋 Connect.	Configure system filters for logging destin	vetions.				
Find Go						
10.26.2	Logging Destination	Systeps From All Event: Classes		Syslogs From Specific Event Class	в	Edit
- 5 10.106.44.146	SNMP Trap	- Oisatiled				
	Internal Buffer	- Disabled				
Device Management dn #	Constitu	- Disatist -				
- Planagement Selection Que +	Telnet and SSH Sessions	- Disabled				
Paragement Access Rule	ASDM	Disabled				
8-36 Literating	Systog Servers	- Disabled				
B 28 System Image/Configuration						
Pligh Availability and Scalabilit						
- Logging Setup						
-StePhal Setup						
Rate Link						
- Synlog Servers						
a the second second						
A Device Setup						
🕄 Frend						
Remote Access VPV						
🔗 Statu-Statin						
🚖 Irend Micro Content Security						
Device Management						
:			Apply Reset			
				disco 16	10 🖓	0,000 06 7122:20 AMUTC

8. Kies een geschikte ernst, in dit geval **informatie**, uit de vervolgkeuzelijst **Filter op ernst**. Klik op **OK** wanneer u klaar bent.

Edit Logging Filters			×				
Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.							
Logging Destination: Syslog Servers							
Syslogs from All Event Classes							
Filter on severity Informational -							
🔿 Use event list 💿 👻 New							
Disable logging from all event classes							
Syslogs from Specific Event Classes							
	Event Class	Severity					
Event Class: auth							
Description: User Authentication							
Severity: Emergencies -							
OK Car	Help						

9. Klik op **Toepassen** nadat u bent teruggekeerd naar het venster Logging Filters.

Cisco ASDM 7.3 for ASA - 10.306.44	164					- 0 - X
File View Tools Winds Winds	w Help			Тури	topic to search GO	ababa
🕞 Hone 🦓 Carriguestan [Man	koring 🔚 Sove 🔇 Rehesh 🔇 Back I	🕐 Forward 💡 Help				CISCO
Device List d1 4 ×	Configuration > Device Management >	Logging > Logging filters				
🗣 Add 🁔 Delete 🖋 Correct.	Configure syslog filters for logging destinatio	ns.				
Find Go						
10.105.44.144	Logging Destination	Syslogs From All Event: Oasses		Syslogs/Fran Specific Event Classes		Lik
- 310.106.44.146	SNMP Trap	- Oisabled				
10.106.44.178	Internal Buffer	Disabled				
Device Management (1) +	E-Mol	- Oisatiled				
- Paragement Sealon Qut +	Controller Takent and FTM Factions	- Deadled				
-TT 50000	ASTM	- Ceaded				
The Statement Access Rule	Sydog Servers	Severity: Informational				
B 3 System Image/Configuration						
🗄 🥑 High Availability and Scalabilit						
D Loging						
Logging Setup						
E-Piel Setup						
Electric fibers						
Rate Lint						
- Syslag Servers						
A IN A IN A						
2 Caulta Calua						
Contraction of the						
🖏 ryssal						
Bemake Access VPN						
🚰 Steits-Ste UN						
A Irend Micro Content Security						
Device Management						
:			Apply Reset			
				disco 15	10,00	066 7129130 AMUTC

Verzend Syslog-berichten via VPN naar een Syslog-server

In het eenvoudige VPN-ontwerp van site-to-site of in het gecompliceerdere hub-and-spoke ontwerp zou de beheerder alle externe ASA-firewalls kunnen bewaken met de SNMP-server en syslog-server op een centrale site.

Raadpleeg <u>PIX/ASA 7.x</u> en hoger om de IPsec VPN-configuratie van site-to-site te configureren: voorbeeld

van configuratie van PIX-to-PIX VPN-tunnel. Naast de VPN-configuratie moet u de SNMP en het interessante verkeer voor de syslogserver configureren op zowel de centrale als de lokale site.



Configuratie centrale ASA

<#root>

!--- This access control list (ACL) defines IPsec interesting traffic. !--- This line covers traffic between the LAN segment behind two ASA. !--- It also includes the SNMP/syslog traffic between the SNMP/syslog server !--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161 access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161 access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162 access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162 access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514

logging enable logging trap debugging

!--- Define logging host information.

logging facility 16 logging host inside 172.22.1.5

!--- Define the SNMP configuration.

snmp-server host inside 172.22.1.5 community ***** version 2c

ASA-configuratie op afstand

<#root>

!--- This ACL defines IPsec interesting traffic. !--- This line covers traffic between the LAN segment behind two ASA. !--- It also covers the SNMP/syslog traffic between the SNMP/syslog server !--- and the network devices located on the Ethernet segment behind ASA 5515. access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0 !--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and !--- syslog traffic (UDP port - 514) sent from this ASA outside !--- interface to the SYSLOG server. access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161 access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161 access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162 access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162 access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514 !--- Define syslog server. logging facility 23 logging host outside 172.22.1.5

!--- Define SNMP server.

snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****

Raadpleeg <u>Cisco Secure ASA Firewall met SNMP en Syslog via VPN-tunnel controleren</u> voor meer informatie over de configuratie van ASA versie 8.4

Geavanceerde systeemsleuf

ASA versie 8.4 biedt verschillende mechanismen waarmee u syslog-berichten in groepen kunt configureren en beheren. Deze mechanismen omvatten het niveau van de berichtstrengheid, berichtklasse, bericht-ID, of een lijst van het douanebericht die u creeert. Met behulp van deze mechanismen kunt u één opdracht invoeren die van toepassing is op kleine of grote groepen berichten. Wanneer u op deze manier syslogs instelt, kunt u de berichten van de opgegeven berichtgroep opnemen en niet meer alle berichten van dezelfde ernst.

Gebruik de Berichtenlijst

Gebruik de berichtenlijst om alleen de geïnteresseerde syslog-berichten op prioriteitsniveau en ID in een groep op te nemen, dan associeer deze berichtenlijst met de gewenste bestemming.

Voltooi deze stappen om een berichtlijst te configureren:

- 1. Typ de **logboeklijst** *message_list | level severity_level [class message_class]* opdracht om een berichtenlijst te maken die berichten bevat met een bepaald prioriteitsniveau of berichtenlijst.
- 2. Voer de opdracht *message_list* message *syslog_id-syslog_id2 in* om extra berichten toe te voegen aan de lijst met berichten die zojuist zijn gemaakt.
- 3. Voer de **opdracht** *message_list* van de **logboekbestemming in** om de bestemming van de gemaakte berichtenlijst op te geven.

Voorbeeld 2

Voer deze opdrachten in om een berichtenlijst te maken die alle essentiële 2-berichten bevat met de toevoeging van 611101 aan 611323, en u kunt deze ook naar de console laten sturen:

<#root>

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

ASDM-configuratie

Deze procedure toont een ASDM-configuratie voor voorbeeld 2 met het gebruik van de berichtenlijst.

1. Kies de Lijsten van de Gebeurtenis onder Vastlegging en klik Add om een berichtlijst te creëren.

Cisco ASDM 7.1 for ASA - 10.106.44	144								- 0 - X -
File View Tools Wigards Winds	ow Help						Type topic to search	Go	alada
🕞 Hone 🦓 Cantage asson 📴 Mar	itoing 🔚 Sove 🔇 Refe	sh 🕓 Back 💟 Forward	🤪 HAD						cisco
Device List dr. 9 ×	Configuration > Device M	lanagement > Logging > Ex	enk Lista						
🕈 Add 📋 Delete 🖋 Connect.	Use event lists to define a	particular set of syslogs that yo	are interested in. The event list ca	be used to filter syslogs s	sent to a logging des	bination .			
Find Go									
- 5 10.2.6.2 A 10.105.44.144 - 5 10.105.44.146 - 5 10.105.44.176 *	None		Event Oass (Sevenity			Nessage IIIs			Add E.St. Delete
Comparent Senior Cur + Stel Senior Cur + Stel Senior Cur + Stel Senior Cur + Senior Cur +									
Conjung There Synlog Servers									
Brenche Access VPV Brenche Access VPV Brenche Stee VPN Dente Visro Cantent Security Dente Visrogement									
:				Apply R	leset				
					de	10 15	10 👰	6 10,0	8/06 7130-20 AMUTC

2. Voer in het veld Naam de naam in van de berichtenlijst. In dit geval wordt **my_critical_message** gebruikt. Klik op **Add** onder Event Class/Severity Filters.

Add Event List	:			
lame: my_critica	I_messages			
pecify filters for I epresents the ma o the specified let	the event list. You aximum level for lo vel.	ı can filter syslogs by gging messages. The	their class and severity, or by th ASA will filter system log messag	eir IDs. The severity leve es with severity levels up
vent Class/Sever	rity Filters ———		Message ID Filters	
Event Class	Severity	Add	Message IDs	Add
		Edit		Edit
		Delete		Delete
L		ок са	ancel Help	

3. Kies **Alles** uit de vervolgkeuzelijst Event Class. Kies **Kritisch** in de vervolgkeuzelijst Ernst. Klik op **OK** wanneer u klaar bent.

	🔁 Add Class and Severity Filter
	Event Class: 🔄 All 💌
l	Description: All Event Classes
	Severity:
	OK Cancel Help

4. Klik op **Add** onder de filters Message ID als er extra berichten nodig zijn. In dit geval moet u berichten in met ID 611101-611323.

🧧 Add Event List			×				
Name: my_critical_messages							
Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs. The severity level represents the maximum level for logging messages. The ASA will filter system log messages with severity levels up to the specified level.							
Event Class/Severity Filters	M	essage ID Filters					
Event Class Severity	Add	Message IDs	Add				
All Critical	Edit		Edit				
	Delete		Delete				
	OK Cancel	Help					

5. Plaats het bereik van de ID in het vak Berichten-ID's en klik op **OK**.

🔁 Add Syslog	Message ID Filter	×
Enter the sysic of sysiog IDs, I	ng message ID. Use hyphen to specify a for example, 101001-101010.	range
Message IDs:	611101-611323	
	K Cancel Help	

- 6. Ga terug naar het menu Filters vastlegging en kies console als bestemming.
- 7. Kies my_critical_message uit de vervolgkeuzelijst Use event list. Klik op OK wanneer u klaar bent.

Edit Logging Filters	And and the second			×		
Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.						
Logging Destination: Sy:	slog Servers					
Syslogs from All Event C	lasses					
💿 Filter on severity	Informational 🚽					
 Use event list 	my_critical_messages 👻 New					
🔘 Disable logging fro	om all event classes					
Syslogs from Specific Eve	ent Classes					
		Event Class	Severity			
Event Class: auth	▼ Add >>					
Description: User A	Authentication					
Severity: Emer	gencies 🗸					
OK Cancel Help						

8. Klik op Toepassen nadat u bent teruggekeerd naar het venster Logging Filters.

Cisco ASDM 7.3 for ASA - 10.308.44	144 or hangin likes had been been	defaulte a test a second				- 0 - X
File View Tools Wgards Windo	w Help				Type topic to search	🔍 սիսիս
🕤 Hore 🖧 Configuration 🔯 Mon	Roing 🔚 Sove 🔇 Rehesh 🔇 Back	C Forward 💡 Help				CISCO
Device List d ¹ P ×	Configuration > Device Management >	Logging > Logging filters				
🗢 Add 📋 Delete 🖉 Correct.	Configure syslog filters for logging destinat	ians.				
Find Go						
10.2.6.2 ·	Logging Destination	Syslogs From All Event: Classes		Syslogs:Fran Specific Event Classes		Edit
- 30.106.44.146	SNMP Trap	- Oisatiled				
- 5 10.105.44.175	Internal Buffer	Disabled				
Device Management dn #	Constitu	- Dealed -				
- Planagement Selection Qut: A	Telnet and SSH Sessions	- Disabled				
Paragement Access Rule	ASDM	Disabled				
8-86 Literating	Systog Servers	Event List: my_pilical_ness	ages			
B-30 System Inage/Configuration						
E Leastro						
- Digging Setup						
-Statistics						
Event Lata						
Rate Link						
- Synlog Servers						
A The Province Section						
Device Setup						
🕰 Frend						
Bemake Access WPW						
Statu-Sta UN						
A Irend Micro Content Security						
Texts Hereswert						
:			Apply Reset			
Configuration changes saved successfully.				disco 15	III 🖉 🖬 🔰 🖆	10,02006 9129:10 AMUTC

Hiermee zijn de ASDM-configuraties voltooid met behulp van een berichtenlijst zoals in voorbeeld 2.

De berichtklasse gebruiken

Gebruik de berichtklasse om alle berichten die aan een klasse zijn gekoppeld naar de gespecificeerde uitvoerlocatie te verzenden. Wanneer u een drempel van het strengheidsniveau specificeert, kunt u het aantal berichten beperken die naar de uitvoerlocatie worden verzonden. <#root>

logging class

```
message_class destination | severity_level
```

Voorbeeld 3

Voer deze opdracht in om alle ca-klasseberichten met een prioriteitsniveau van noodgevallen of hoger naar de console te verzenden.

<#root>

logging class ca console emergencies

ASDM-configuratie

Deze procedure toont de ASDM-configuraties bij voorbeeld 3 met het gebruik van de berichtenlijst.

- 1. Kies het menu Filters vastlegging en kies console als bestemming.
- 2. Klik op Logboekregistratie uitschakelen in alle gebeurtenisklassen.
- 3. Kies onder Syslogs uit Specifieke gebeurtenisklassen de klasse en de ernst die u wilt toevoegen.

Deze procedure maakt gebruik van respectievelijk ca en noodgevallen.

4. Klik op Add om dit toe te voegen aan de berichtklasse en klik op OK.

Edit Logging Filters			×			
Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.						
Logging Destination: Console						
Syslogs from All Event Classes						
○ Filter on severity Emergencies						
🔘 Use event list 🛛 my_critical_messages 👻 🔹 New						
Oisable logging from all event classes						
Syslogs from Specific Event Classes						
	Event Class	Severity				
Event Class: iza	auth	Emergencies				
Description: Authority						
Severity: Emergencies -						
	L					
OK Cancel Help						

5. Klik op **Toepassen** nadat u bent teruggekeerd naar het venster Logging Filters. De console verzamelt nu het bericht van de ca-klasse met het niveau van de ernst Noodsituaties zoals getoond in het venster van de Filters van het Vastleggen.

Cisco ASDM 7.1 for ASA - 10.306.44	144					- 0 - X -
File View Tools Wgards Winds	w Help				Type topic to search	60 alsola
🕞 Hore 🖓 Cantagration 🔯 Mar	koing 🔚 Sove 🔇 Refresh 🔇 Bad	C Forward 🦻 Help				CISCO
Device List d ¹ P ×	Configuration > Device Management >	Longing > Longing Filters				0
🗢 Add 📋 Delete 🖉 Connect.	Configure system filters for logging destinat	tions.				
Find 60						
5 30.2.6.2 *	Logging	Syslogs From		Syslags From		Edit
	Destination	All Event Classes		Specific Event Classes		
- 3D.106,44,246	SNMP Trop	Disatiend				
10.106.44.170	Internal Buffer	Disabled				
Device Management dr @	E-Mol	- Disabled				
- Management Seletan Que +	Conscile	Disabled		auth : Creargancies		
5997	Tellet and Soll Sessions	- Osabed				
Paragement Access Rule	Risteri Gudas George	- Dealers - Event its our elited meanage				
B go Loning	System Services	Everena vi _uvca_vesoajes				
- and system anapoptoregunation						
E-E Loging						
Logging Tellup						
- 😽 E-Mail Setup						
- Dvent Liste						
Logging Filters						
Raba Linit						
Synlog Servers *						
4 III +						
0						
B Device Setup						
🕄 Frend						
Benote Access VPN						
Stato-Sta UN						
🚖 Trend Micro Cantent Security						
Device Management						
20 2 2		Apply	Reset			
Configuration changes saved successfully.				disto 15	III 🖉 🔂	10/28/06 9:27:50 AMUTC

Hiermee is de ASDM-configuratie voltooid, bijvoorbeeld 3. Verwijs naar <u>Berichten die door het Niveau van</u> <u>de Ernst</u> voor een lijst van de niveaus van de logboekbericht worden <u>vermeld</u>.

Verzend debug log berichten naar een syslog server

Voor geavanceerde probleemoplossing zijn functie-/protocolspecifieke debug-logbestanden vereist. Standaard worden deze logberichten op de terminal (SSH/Telnet) weergegeven. Afhankelijk van het type van debug, en het tarief van debug geproduceerde berichten, kan het gebruik van CLI moeilijk blijken als debugs wordt toegelaten. Optioneel, debug berichten kunnen worden omgeleid naar het syslog proces en gegenereerd als syslogs. Deze syslogs kunnen worden verzonden naar elke syslogbestemming zoals elke andere syslogg. Als u debugs naar syslogs wilt omleiden, voert u de opdracht **debug-trace voor** het **vastleggen in**. Deze configuratie stuurt debug-uitvoer, als syslogs, naar een syslogserver.

logging trap debugging logging debug-trace logging host inside 172.22.1.5

Gebruik van de Lijst van het Vastleggen en Berichtklassen samen

Voer de opdracht **logboeklijst** in om alleen de syslog voor LAN-to-LAN- en IPsec VPN-berichten met externe toegang op te nemen. In dit voorbeeld worden alle logberichten van het VPN (IKE en IPsec)-klassesysteem met een debugingniveau of hoger opgenomen.

Voorbeeld

```
<#root>
hostname(config)#
logging enable
hostname(config)#
logging timestamp
hostname(config)#
logging list my-list level debugging class vpn
hostname(config)#
logging trap my-list
hostname(config)#
logging host inside 192.168.1.1
```

ACL-treffers in logbestanden

Voeg **logbestand** toe aan elk element van de toegangslijst (ACE) dat u wenst om te registreren wanneer een toegangslijst wordt geraakt. Gebruik deze syntaxis:

access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}

Voorbeeld

<#root>

ASAfirewall(config)#

access-list 101 line 1 extended permit icmp any any log

Standaard worden alle geweigerde pakketten door ACL's geregistreerd. Er is geen behoefte om de logboekoptie toe te voegen om ACLs te **ontkennen** om syslogs voor ontkende pakketten te produceren. Wanneer de **logoptie** is gespecificeerd, wordt syslog-bericht 106100 gegenereerd voor ACE waarop het is toegepast. Syslog-bericht 106100 wordt gegenereerd voor elke overeenkomende vergunning of ontkent ACE-stroom die door de ASA-firewall loopt. De first-match flow wordt gecached. De verdere gelijkenverhoging de klaptelling die in het bevel van de **show toegang-lijst** wordt getoond. Het gedrag bij het vastleggen van de standaardtoegangslijst, dat het niet-opgegeven **logboeksleutelwoord** is, is dat als een pakket wordt ontkend, bericht 106023 wordt gegenereerd en als een pakket is toegestaan, wordt er geen syslogbericht gegenereerd.

Een optioneel syslog niveau (0 - 7) kan gespecificeerd worden voor de gegenereerde syslog berichten (106100). Als er geen niveau is opgegeven, is het standaardniveau 6 (informatie) voor een nieuw ACE. Als ACE reeds bestaat, dan blijft zijn huidige logboekniveau onveranderd. Als de optie **logboekblokkering** is gespecificeerd, is de logboekregistratie volledig uitgeschakeld. Er wordt geen syslogbericht gegenereerd dat bericht 106023 bevat. Met de **logoptie** wordt het logboekgedrag van de standaardtoegangslijst hersteld.

Voltooi deze stappen om het syslogbericht 106100 in de consoleoutput te bekijken:

- 1. Voer de opdracht **Logboekregistratie inschakelen in** om de transmissie van systeemlogberichten naar alle uitvoerlocaties mogelijk te maken. U moet een logboekuitvoerlocatie instellen om logbestanden te kunnen bekijken.
- 2. Voer de opdracht **logboekbericht <message_number>level <severity_level> in** om het prioriteitsniveau van een specifiek systeemlogbericht in te stellen.

Typ in dit geval de opdracht **106100 voor** het **registratiebericht** om bericht 106100 in te schakelen.

- 3. Typ de **logboekconsole message_list** | **de** opdracht **Severity_level** om het mogelijk te maken dat systeemlogberichten op de Security Appliance console (ty) worden weergegeven wanneer ze zich voordoen. Stel severity_level in van 1 tot 7 of gebruik de naam van het niveau. Je kunt ook specificeren welke berichten verzonden worden met de message_list variabele.
- 4. Voer de opdracht **logboekbericht tonen in** om een lijst weer te geven van meldingen in het systeemlogboek die zijn gewijzigd vanuit de standaardinstelling, namelijk berichten die een ander prioriteitsniveau hebben toegewezen en berichten die zijn uitgeschakeld.

Dit is voorbeelduitvoer van de opdracht voor het logboekbericht voor de show:

<#root>

ASAfirewall#

show logging message 106100

```
syslog 106100: default-level informational (enabled)
ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Syslog-generatie blokkeren op een standby ASA

Begin vanaf ASA softwarerelease 9.4.1 en u kunt specifieke systemen blokkeren die op een standby-eenheid worden geproduceerd en dit gebruiken opdracht:

no logging message syslog-id standby

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Als u een specifiek syslog bericht wilt onderdrukken dat naar syslog server moet worden verzonden, dan moet u het bevel invoeren zoals getoond.

<#root> hostname(config)# no logging message <syslog_id>

Raadpleeg de opdracht voor het registratiebericht voor meer informatie.

%ASA-3-201008: nieuwe verbindingen verbieden

De %ASA-3-201008: Uitschakelen van nieuwe verbindingen. foutmelding wordt weergegeven wanneer een ASA geen contact kan opnemen met de syslogserver en er geen nieuwe verbindingen zijn toegestaan.

Oplossing

Dit bericht wordt weergegeven wanneer u TCP-systeemlogberichten hebt ingeschakeld en de syslog-server niet kan worden bereikt, of wanneer u Cisco ASA Syslog Server (PFSS) gebruikt en de schijf op het Windows NT-systeem vol is. Voltooi de volgende stappen om deze foutmelding op te lossen:

- Schakel het logbestand van het TCP-systeem uit als dit is ingeschakeld.
- Als u PFSS gebruikt, maak dan ruimte vrij op het Windows NT-systeem waar PFSS zich bevindt.

- Zorg ervoor dat de syslogserver is geïnstalleerd en u kunt de host pingen vanaf de Cisco ASAconsole.
- Vastlegging TCP-systeembericht opnieuw starten om verkeer toe te staan.

Als de syslogserver uitvalt en de TCP<u>-</u>logboekregistratie is geconfigureerd, gebruikt u de<u>logboeklicentie</u><u>hostdown</u>-opdracht of de switch naar UDP-logboekregistratie.

Cisco ASDM 7.1 for ASA - 10.106.44.	144					
File View Tools Wigards Windo	w Help				Pype topic to search	© alate
🕞 Hore 🦓 Cantauration [Mon	Raing 🔚 Sove 🔇 Refe	sh 🔇 Back. 🔘 Forward 💡 Help				CISCO
Device List dr. 9 ×	Configuration > Device N	lanagement > Logging > Syring Server	a			
🗣 Add 📋 Delete 🖉 Correct.	Specify up to 16 syslop ser	vers. Hake sure logging is enabled in Configu	ration > Device Management > Logging > Logg	ing Setup.		
Find Go						
- 5 1D.2.6.2	Interface	IP Address	Protocol/Port	EHBLEM	Secure	Add
- 5 30.106.44.346	reide	172.224.6	U04/524	No	No	1.2
10.106.44.178 *						Delete
Device Management d1 =						
Management Access Rules						
38 System Inage/Configuration						
- Auto Update						
Boot Image/Configuration State Evaluation						
Loopho						
-By Logging Setup						
- De Logging Filters						
False Dreft						
The Station System						
B Devke Setup						
C. Frend						
Hericke Access WHV						
Statu-Station	Specify the number of mea	rages that are allowed to be guezed when a	ryolog server is busy. Use Dito indicate unlevite	d-quantum nizm.		
A Trend Micro Content Security	Queue Ster: 512					
	📝 Alov user traffic to pa	is when TCP systing server is down				
BN Device Management						
:			Apply	Reset		
Configuration changes saved successfully.				dista	15 🔤 🎉 🔝	5/9/14 10:46:02 AMUTC

Gerelateerde informatie

- <u>Referenties voor Cisco Secure PIX-firewall-opdracht</u>
- <u>Requests for Comments (RFC's</u>)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.