

#Configurazione# Impostare un avviso mail su NGAF

***Prodotto:** NGAF

***Versione:** 8.0.85

*1. Introduzione

1.1 Scenario

Identificare accessi non autorizzati sul firewall è fondamentale. Nella seguente guida, vedremo come impostare un avviso mail quando tale evento succede su Sangfor NGAF.

1.2 Requisiti

1. Nella rete dell'utente vi dev'essere un firewall NGAF configurato.
2. è necessario avere un indirizzo di posta funzionante ed i relativi parametri SMTP.

*2. Configurazione

In questa guida useremo un relay smtp interno per inviare mail.

2.1 Configurazione NGAF

Passo 1. Configurare le impostazioni del server email su NGAF

Per far ciò, dovete recarvi nell'interfaccia web di NGAF al seguente punto:

System > Email & SMS Server > Specified Email Server

Network Secure Platform 8.0.85

Home SOC Monitor Policies Objects Network **System**

System

General Settings

Web UI

Network

Email & SMS Server

System Time

NTP Key

HOSTS

Licensing

OOBM

Privacy Options

Security Capability Update

Troubleshooting

Email & SMS Server

Email Server

Specified Email Server ⓘ Built-in Email Server ⓘ

Sender Address:

SMTP Server:

Encryption: ⓘ

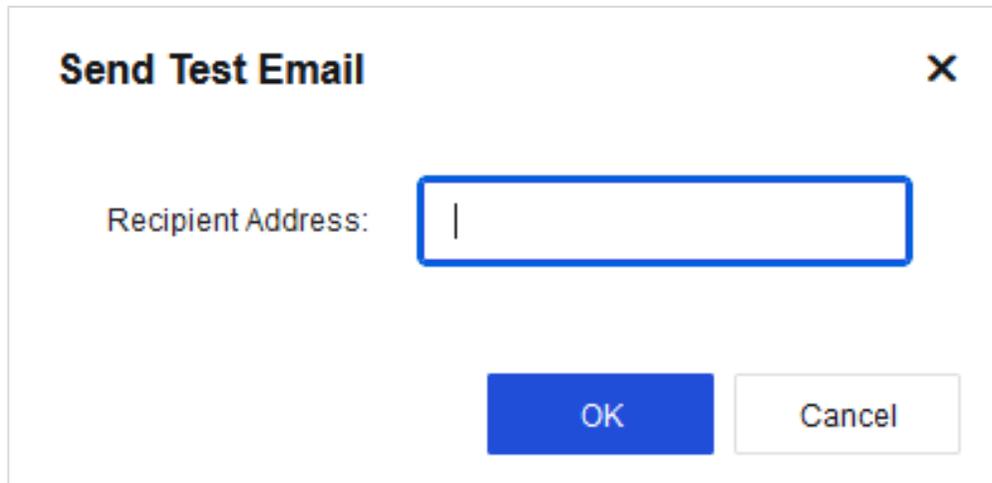
Server Port:

Username:

Password: ⓘ

To specify the recipient address, go to [Monitor > Settings > Alert Notification Settings > Notification Settings](#).

In questa sezione potete aggiungere le impostazioni mail (in questo esempio, viene usato un relay smtp interno, ma da nostri test, abbiamo verificato che funziona molto bene con Microsoft 365) ed effettuare un invio mail di prova cliccando sul bottone Send Test Email specificando un indirizzo di destinazione:



The image shows a dialog box titled "Send Test Email" with a close button (X) in the top right corner. Below the title, there is a label "Recipient Address:" followed by a text input field with a blue border and a vertical cursor. At the bottom of the dialog, there are two buttons: a blue "OK" button and a white "Cancel" button with a grey border.

Nella casella mail di destinazione, controllate attentamente che la mail di test non finisca in spam.

Passo 2. Per specificare l'indirizzo di destinazione degli avvisi mail sul firewall Sangfor NGAF, recarsi nell'interfaccia web alla seguente sezione

Monitor > Settings > Alert Notification Settings > Notification Settings

The screenshot displays the Network Secure Platform interface. At the top, the navigation bar includes the logo, version number (8.0.85), and menu items: Home, SOC, Monitor (highlighted), Policies, Objects, Network, and System. Below the navigation bar, the page title is "Email & SMS Server". The left sidebar contains a menu with items: Monitor, Logs, Top N, Sessions, Statistics, Report, Diagnosis, Settings, Logging Options, and Top N Options. The "Alert Notification Settings" item is highlighted in blue. The main content area is divided into two tabs: "Event Settings" and "Notification Settings" (selected). A yellow warning banner at the top of the main content area states: "SMS alert messages cannot be received because SMS server is not configured. [Configure Now](#)". Below the banner, the "Email Alert" section contains the following fields: "Email Subject" with the value "[Sangfor NGAF Alert]", "Email Address" with a text area containing "One entry per row, Number of email addresses cannot exceed 5.", and "Interval (mins):" set to "Every 20 minutes". The "SMS Alert" section contains an "SMS template ID" field. A note below this field reads: "Note: You need to copy the following SMS template to the SMS service provider for review and obtain the ID."

In questo punto è possibile impostare un indirizzo mail di destinazione e l'oggetto da usare (quest'ultima impostazione è utile qualora vi siano delle regole applicate sulla cassetta postale di destinazione che raggruppano tutte le mail con uno specifico oggetto in una determinata sotto cartella).

Passo 3. Nel tab Event Settings è necessario abilitare globalmente gli avvisi cliccando su Enable alert notifications

The screenshot displays the Network Secure Platform interface. At the top, the navigation bar includes the logo, version number (8.0.85), and menu items: Home, SOC, Monitor (highlighted), Policies, Objects, Network, and System. Below the navigation bar, the page title is "Email & SMS Server". A dark sidebar on the left contains the following menu items: Monitor, Logs, Top N, Sessions, Statistics, Report, Diagnosis, Settings (expanded), Logging Options, Top N Options, and Alert Notification Settings (highlighted). The main content area is titled "Event Settings" and "Notification Settings". It features a checkbox for "Enable alert notifications" which is currently unchecked. Below this, there are three sections: "Basics:", "High Availability:", and "Business Resources:". Each section has an "Enable" checkbox checked. The "Basics:" section contains a list of events with checkboxes: Admin login failure, Monitoring object anomaly, License expiration, SMTP server change, Process faults, Time inconsistency, and Admin username and. The "High Availability:" section contains "High Availability". The "Business Resources:" section contains "Port resource overload".

Passo 4. A questo punto, selezionare solamente gli eventi cui volete ricevere un avviso via mail. In questo esempio, selezioneremo l'avviso Admin login failure dato che si vuole avere un avviso quando si verifica un accesso non autorizzato con l'utenza amministrativa:

Event Settings Notification Settings

Enable alert notifications

Basics: Enable

- Admin login failure
- Monitoring object anomaly
- License expiration
- SMTP server change
- Process faults
- Time inconsistency
- Admin username and

2.2 Eseguire un test di login amministrativo fallito

Passo 1. A questo punto, è possibile far scattare l'avviso simulando un accesso fallito con l'utenza amministrativa sull'interfaccia web del firewall.



Network Secure Platform

Version: Network Secure 8.0.85 IPv6

Username or password is incorrect, you have 7 attempts left

Username

admin

Password

Passo 2. È possibile verificare il login fallito nell'interfaccia web del firewall in questa sezione:

Monitor > System Logs > Admin Operation Logs

É possibile effettuare una ricerca usando il filtro predefinito al fine di visualizzare il login fallito con l'utenza amministrativa

No.	Admin	Account Type	Mgmt Method	Host IP	Object	Operation	Time	Description	Details
1	admin	Local user	Web UI	10.0.1.32	Username	Log in to web UI	2024-03-21 13:37:51	UsernameLog in to web UI Failed: Username or password is incorrect...	View

No.1

Admin: admin
Account Type: Local user
Management Method: Web UI
Host IP: 10.0.1.32
Object: Username
Operation: Log in to web UI
Time: 2024-03-21 13:37:51
Description: UsernameLog in to web UI Failed: Username or password is incorrect, you have 8 attempts left.admin

*3. Attenzione

1. Tenere a mente che, se si vuole usare Microsoft 365 come server SMTP, dovete configurare le seguenti impostazioni inerenti il server SMTP:

System > Email & SMS Server > Specified Email Server

The screenshot shows the configuration page for the Email & SMS Server in the Network Secure Platform. The interface includes a top navigation bar with tabs for Home, SOC, Monitor, Policies, Objects, Network, and System. A left sidebar contains a menu with options like System, General Settings, Web UI, Network, Email & SMS Server (highlighted), System Time, NTP Key, HOSTS, Licensing, OOBM, and Privacy Options. The main content area is titled 'Email & SMS Server' and features a sub-section 'Email Server' with two radio buttons: 'Specified Email Server' (selected) and 'Built-in Email Server'. Below these are several input fields: 'Sender Address' (empty), 'SMTP Server' (smtp.office365.com), 'Encryption' (StartTLS), 'Server Port' (587), 'Username' (empty), and 'Password' (masked with dots). A 'Send Test Email' button is located at the bottom of the configuration area.

Network Secure Platform 8.0.85 Home SOC Monitor Policies Objects Network System

Email & SMS Server System Logs

Email & SMS Server

Email Server

Specified Email Server ⓘ Built-in Email Server ⓘ

Sender Address:

SMTP Server:

Encryption: ⓘ

Server Port:

Username: ⓘ

Password: ⓘ