

#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

The screenshot displays the 'Network Secure Platform' interface. The top navigation bar includes links for Home, SOC, Monitor, Policies, Objects, Network, and System (which is highlighted). The left sidebar contains a menu with System, General Settings, Web UI, Network, Email & SMS Server (highlighted), System Time, NTP Key, HOSTS, Licensing, OOBM, Privacy Options, Security Capability Update, and Troubleshooting. The main content area is titled 'Email & SMS Server' and features two radio buttons: 'Specified Email Server' (selected) and 'Built-in Email Server'. Below these are input fields for Sender Address, SMTP Server, Encryption (set to None), Server Port (set to 25), Username, and Password. A 'Send Test Email' button is located at the bottom of the form. A note at the bottom of the page states: 'To specify the recipient address, go to Monitor > Settings > Alert Notification Settings > Notification Settings.'

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: ⓘ

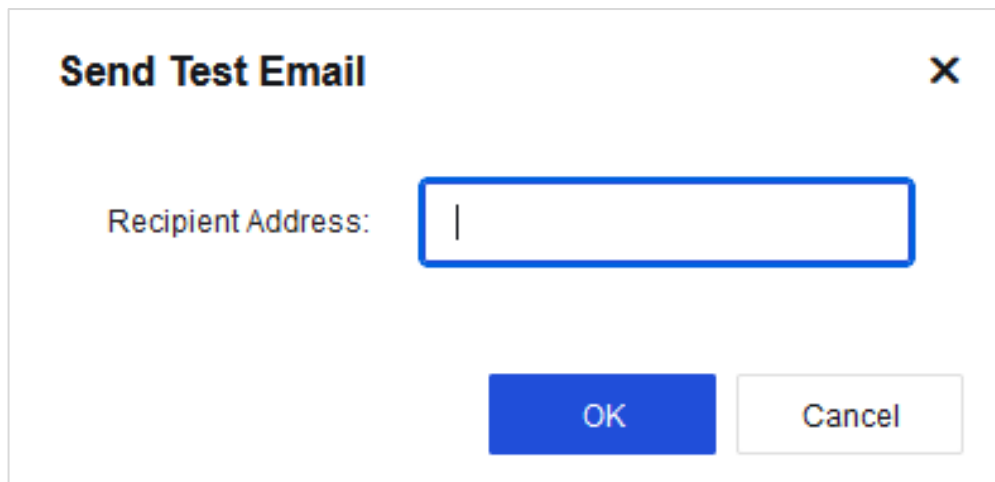
Server Port:

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:

A dialog box titled "Send Test Email" with a close button (X) in the top right corner. It contains a label "Recipient Address:" followed by a text input field with a blue border. At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

Send Test Email X

Recipient Address:

OK Cancel

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

Network Secure Platform8.0.85

HomeSOCMonitorPoliciesObjectsNetworkSystem

Email & SMS Server

Monitor

Logs

Top N

Sessions

Statistics

Report

Diagnosis

Settings

Logging Options

Top N Options

Alert Notification Settings

Event Settings

Notification Settings

SMS alert messages cannot be received because SMS server is not configured. [Configure Now](#)

Email Alert

Email Subject:

[Sangfor NGAF Alert]

Email Address:

One entry per row.,Number of email addresses cannot exceed 5.

Interval (mins):

Every

20

minutes

SMS Alert

SMS template ID:

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

Network Secure Platform 8.0.85 Home SOC Monitor Policies Objects Network System

Email & SMS Server

Monitor

- Logs
- Top N
- Sessions
- Statistics
- Report
- Diagnosis
- Settings
 - Logging Options
 - Top N Options
 - Alert Notification Settings

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

High Availability: ☒ Enable

- ☒ High Availability

Business Resources: ☒ Enable

- ☒ 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

☒ Process faults

☒ Monitoring object anomaly

☒ Time inconsistency


☒ License expiration

☒ Admin username and

☒ SMTP server change

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

Network Secure Platform 9.9.85

HomeSOCMonitorPoliciesObjectsNetworkSystem

Menu name

Email & SMS Server

System LogsAlert Notification Settings

Monitor

Logs

Security Logs

Access Logs

System Logs

Admin Operation LogsSystem Security LogsLocal ACL Logs

Filter | Export Logs | Refresh

Filter: Period (2024-03-21 00:00 - 2024-03-21 23:59) | Admin (Users) | Account Type (All) | Management Method (All) | Object (All) | Description (-)

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 'Network Secure Platform' interface with version 8.0.85. The top navigation bar includes links for Home, SOC, Monitor, Policies, Objects, Network, and a highlighted 'System' button. Below this, a breadcrumb trail shows 'Email & SMS Server' and 'System Logs'. The left sidebar contains a menu with 'System' (selected), '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 contains the 'Email Server' configuration section. This section has two radio buttons: 'Specified Email Server' (selected) and 'Built-in Email Server'. Below the radio buttons are several input fields: 'Sender Address' (empty), 'SMTP Server' (filled with 'smtp.office365.com'), 'Encryption' (dropdown menu showing 'StartTLS' with an information icon), 'Server Port' (filled with '587'), 'Username' (empty with an information icon), and 'Password' (masked with dots with an information icon). At the bottom of this section is a 'Send Test Email' button.

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: ⓘ

Send Test Email