

Feed IoC del CERT-AgID su Firewall pfSense

| | |
|--|--------------------------------|
| Guida realizzata da Data di pubblicazione | Comune di Pescia 19/07/2021 |
|--|--------------------------------|

Procedura per la configurazione del flusso di Indicatori di compromissione (IoC) del CERT-AgID¹ sul Firewall pfSense per la protezione della Pubblica Amministrazione

¹ <https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/>

Indice generale

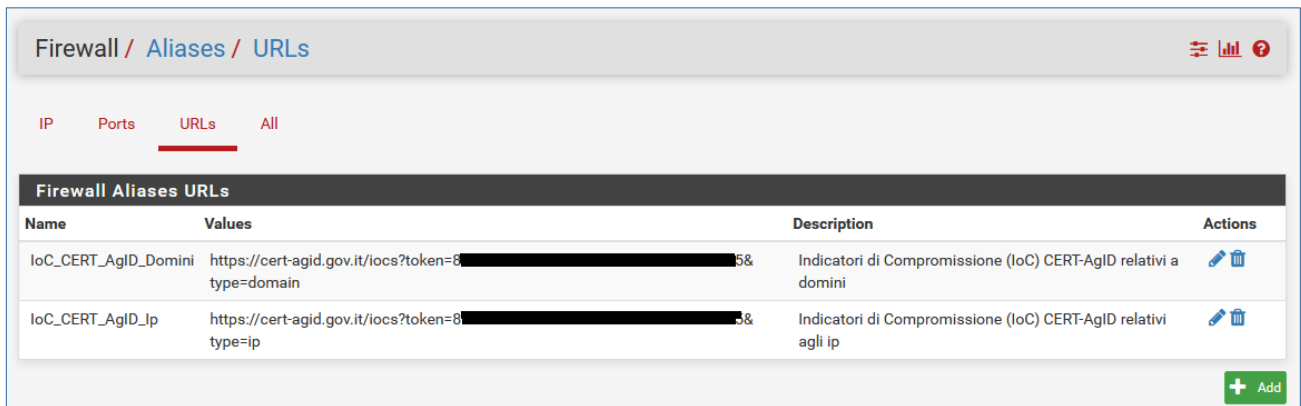
| | |
|---|---|
| Creazione degli Aliases..... | 3 |
| Per i domini..... | 4 |
| Per gli IP..... | 4 |
| Nota per le URL..... | 4 |
| Creazione delle Rules..... | 5 |
| Interfaccia WAN..... | 5 |
| Creare una regola per bloccare gli indirizzi IP sull'interfaccia Wan..... | 5 |
| Creare una regola per bloccare i domini sull'interfaccia Wan..... | 5 |
| Interfaccia LAN:..... | 6 |
| Creare una regola per bloccare gli indirizzi ip sull'interfaccia Lan..... | 6 |
| Creare una regola per bloccare i domini sull'interfaccia Lan..... | 6 |

Creazione degli Aliases

Creare due alias, uno per i domini e uno per gli IP, che serviranno successivamente per creare le regole.

Questo perché gli alias che fanno riferimento ad un URL che espone un elenco di record vengono interpretati da pfSense che ne estrae i valori e li importa in una sua tabella interna.

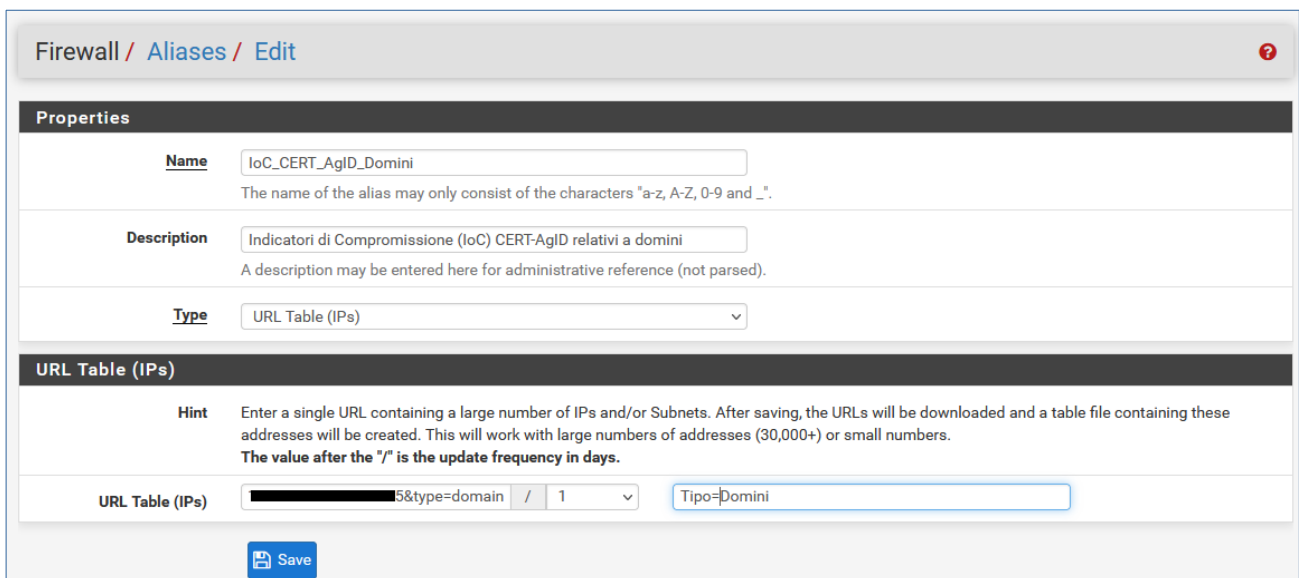
Firewall - Aliases - Urls - Add:



The screenshot shows the 'Firewall / Aliases / URLs' page. At the top, there are tabs for 'IP', 'Ports', 'URLs', and 'All', with 'URLs' selected. Below the tabs is a table titled 'Firewall Aliases URLs' with columns for Name, Values, Description, and Actions. Two entries are listed:

| Name | Values | Description | Actions |
|----------------------|--|--|-----------------|
| IoC_CERT_AgID_Domini | https://cert-agid.gov.it/iocs?token=8[redacted]5&type=domain | Indicatori di Compromissione (IoC) CERT-AgID relativi a domini | [Edit] [Delete] |
| IoC_CERT_AgID_Ip | https://cert-agid.gov.it/iocs?token=8[redacted]5&type=ip | Indicatori di Compromissione (IoC) CERT-AgID relativi agli ip | [Edit] [Delete] |

An '+ Add' button is located at the bottom right of the table.



The screenshot shows the 'Firewall / Aliases / Edit' page. The 'Properties' section contains the following fields:

- Name:** IoC_CERT_AgID_Domini. Below the field, it says: 'The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".'
- Description:** Indicatori di Compromissione (IoC) CERT-AgID relativi a domini. Below the field, it says: 'A description may be entered here for administrative reference (not parsed).'
- Type:** URL Table (IPs) (selected from a dropdown menu).

The 'URL Table (IPs)' section contains a 'Hint' and a form:

Hint: Enter a single URL containing a large number of IPs and/or Subnets. After saving, the URLs will be downloaded and a table file containing these addresses will be created. This will work with large numbers of addresses (30,000+) or small numbers. The value after the "/" is the update frequency in days.

The form has two input fields: 'URL Table (IPs)' containing 'https://cert-agid.gov.it/iocs?token=8[redacted]5&type=domain / 1' and 'Tipo=Domini'. A 'Save' button is at the bottom.

Per i domini

- **Nome**= assegnare un nome
- **Descrizione**=assegnare una descrizione
- **Type**="URL Table (IPs)"
- **URL Table (IPs)**=inserire l'url fornito e filtrato per domini (per filtrare per domini aggiungere al termine dell'url la stringa &type=domain)
- **Impostare il tempo di refresh**, nell'immagine di esempio l'elenco viene aggiornato ogni 1 giorni.

Dopo aver salvato, pfSense convertirà i domini in indirizzi IP, questo richiederà diverso tempo e potrebbe generare un errore di Gateway Timeout, questo è il motivo per cui è preferibile creare due alias separati in modo da ridurre il tempo di elaborazione.

Per gli IP

- o **Nome**= assegnare un nome
- o **Descrizione**=assegnare una descrizione
- o **Type**="URL Table (IPs)"
- o **URL Table (IPs)**=inserire l'url fornito filtrato per gli IP (per filtrare aggiungere al termine dell'url la stringa &type=ip)
- o **Impostare il tempo di refresh**, es. ogni 1 giorni

Nota per le URL

Di default pfSense non accetta alias di link a url specifici. Probabilmente è possibile farlo installando dei packages dedicati (*pfBlocklist*, *pfBlockerNG-devel*) ma si è preferito evitare di installare pacchetti extra per non aumentare il rischio di potenziali problemi durante l'aggiornamento (pfSense consiglia di disabilitarli prima di qualsiasi aggiornamento), inoltre questi pacchetti potrebbero introdurre bug nell'infrastruttura.

N.B.: dopo avere salvato le modifica confermare cliccando su **Apply changes**.

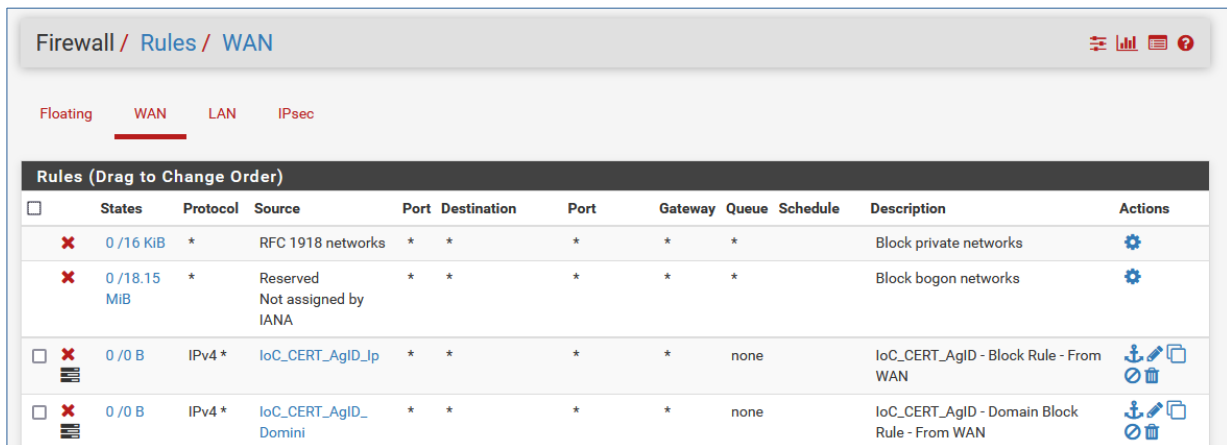
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Creazione delle Rules

Interfaccia WAN

Impostare questa regola per bloccare le minacce in arrivo dall'interfaccia WAN
Dal menu *Firewall - Rules - WAN*:



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules on the WAN interface. The breadcrumb navigation is 'Firewall / Rules / WAN'. There are tabs for 'Floating', 'WAN', 'LAN', and 'IPsec', with 'WAN' selected. Below the tabs is a table titled 'Rules (Drag to Change Order)'. The table has columns for 'States', 'Protocol', 'Source', 'Port', 'Destination', 'Port', 'Gateway', 'Queue', 'Schedule', 'Description', and 'Actions'. There are four rules listed:

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---------------|----------|-------------------------------|------|-------------|------|---------|-------|----------|--|---------|
| 0 / 16 KIB | * | RFC 1918 networks | * | * | * | * | * | * | Block private networks | ⚙️ |
| 0 / 18.15 MiB | * | Reserved Not assigned by IANA | * | * | * | * | * | * | Block bogon networks | ⚙️ |
| 0 / 0 B | IPv4 * | IoC_CERT_AgID_Ip | * | * | * | * | none | | IoC_CERT_AgID - Block Rule - From WAN | 📌 🗑️ |
| 0 / 0 B | IPv4 * | IoC_CERT_AgID_Domini | * | * | * | * | none | | IoC_CERT_AgID - Domain Block Rule - From WAN | 📌 🗑️ |

Creare una regola per bloccare gli indirizzi IP sull'interfaccia Wan

Action = Block;

Interface = WAN;

Address Family = IPv4;

Protocol = Any;

Source = "Single host or alias" -> "Nome Alias IP" [es. IoC_CERT_AgID_Ip]

Destination = Any

Creare una regola per bloccare i domini sull'interfaccia Wan

Action = Block;

Interface = WAN;

Address Family = IPv4;

Protocol = Any;

Source = "Single host or alias" -> "Nome Alias Domini" [es. IoC_CERT_AgID_Domain]

Destination = Any

Interfaccia LAN:

Impostare questa regola per bloccare le minacce in partenza dall'interfaccia LAN
Dal menu *Firewall - Rules - LAN*.

Creare una regola per bloccare gli indirizzi ip sull'interfaccia Lan

Action = Block;

Interface = LAN;

Address Family = IPv4;

Protocol = Any;

Source = Any;

Destination = "Single host or alias" -> "Nome Alias IP" [es. loC_CERT_AgID_Ip]

Creare una regola per bloccare i domini sull'interfaccia Lan

Action = Block;

Interface = LAN;

Address Family = IPv4;

Protocol = Any;

Source = Any;

Destination = "Single host or alias" -> "Nome Alias Domini" [es. loC_CERT_AgID_Domain]

Posizionare le regole subito dopo le regole di default.

Portando il mouse sul nome dell'alias nella colonna Source delle regole WAN si può vedere come la regola applicata ad un alias faccia riferimento ai valori contenuti nell'alias, come mostrato nell'immagine seguente:

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The 'Rules (Drag to Change Order)' table is visible, showing two rules with source aliases 'loC_CERT_AgID_Ip' and 'loC_CERT_AgID_Domini'. The 'Alias details' sidebar on the right shows the IP addresses associated with the 'loC_CERT_AgID_Ip' alias.

| States | Protocol | Source |
|-------------|-------------|----------------------------------|
| 0/16 KiB | * | RFC 1918 networks |
| 0/18.15 MiB | * | Reserved Not assigned by IANA |
| 0/0 B | IPv4 TCP | loC_CERT_AgID_Ip |
| 0/0 B | IPv4 TCP | loC_CERT_AgID_Domini |

Alias details

<https://cert-agid.gov.it/iocs?token=...5&type=ip>

- 1.161.101.20
- 1.161.104.31
- 1.161.122.145
- 1.161.123.180
- 1.234.2.232
- 1.234.21.73
- 2.34.12.8
- 2.50.4.57
- 2.50.137.23
- 2.50.137.155
- 3.215.110.66
- 5.9.116.246
- 5.32.41.45
- 5.54.53.124
- 5.56.132.177
- 5.101.0.44
- 5.193.138.70
- 5.203.199.157
- 5.253.30.17
- 5.255.88.88
- 5.255.88.88
- 5.255.88.88

Disclaimer: il contenuto di questo documento è stato testato e verificato sulla versione PfSense 2.4.5-RELEASE-p1 ed è liberamente distribuibile e modificabile, ma viene rilasciato SENZA ALCUNA GARANZIA.