Feed IoC del CERT-AgID su Firewall pfSense

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

Procedura per la configurazione del flusso di Indicatori di compromissione (IoC) del CERT-AgID[1] sul Firewall pfSense per la protezione della Pubblica Amministrazione

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

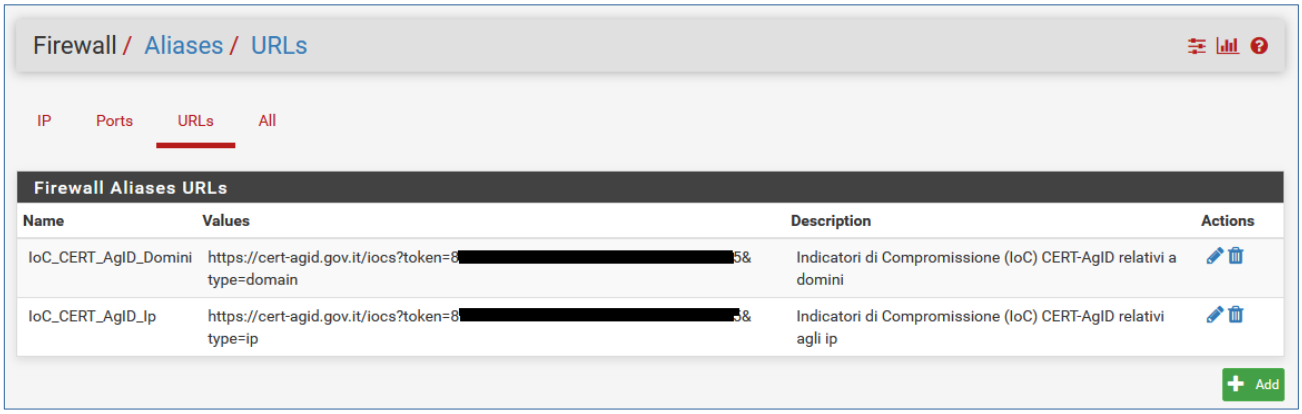
Indice generale

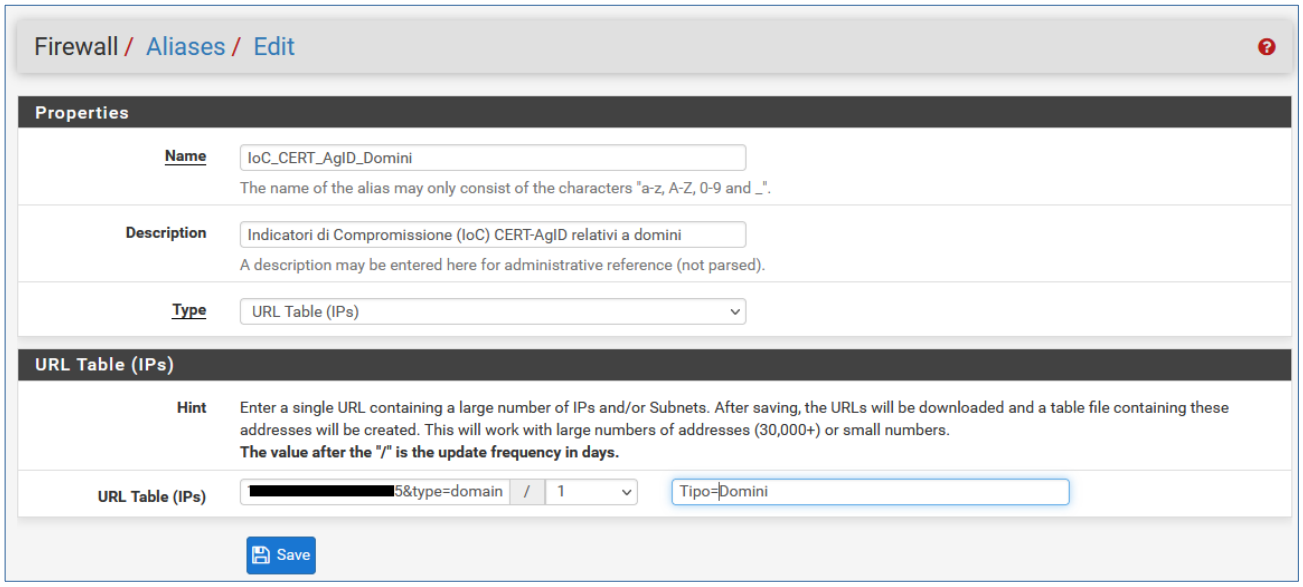
Creazione degli Aliases

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:





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.

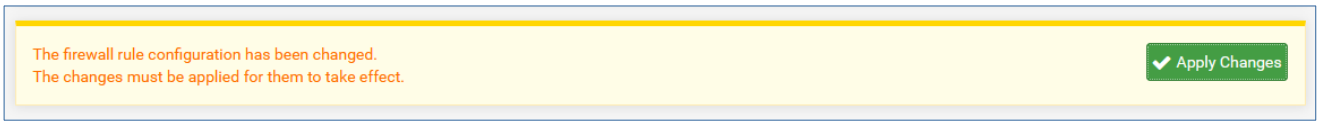
Per gli IP

- **Nome**= assegnare un nome
- **Descrizione**=assegnare una descrizione
- **Type**=”URL Table (IPs)”
- **URL Table (IPs)**=inserire l’url fornito filtrato per gli IP (per filtrare aggiungere al termine dell’url la stringa &type=ip)
- **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.

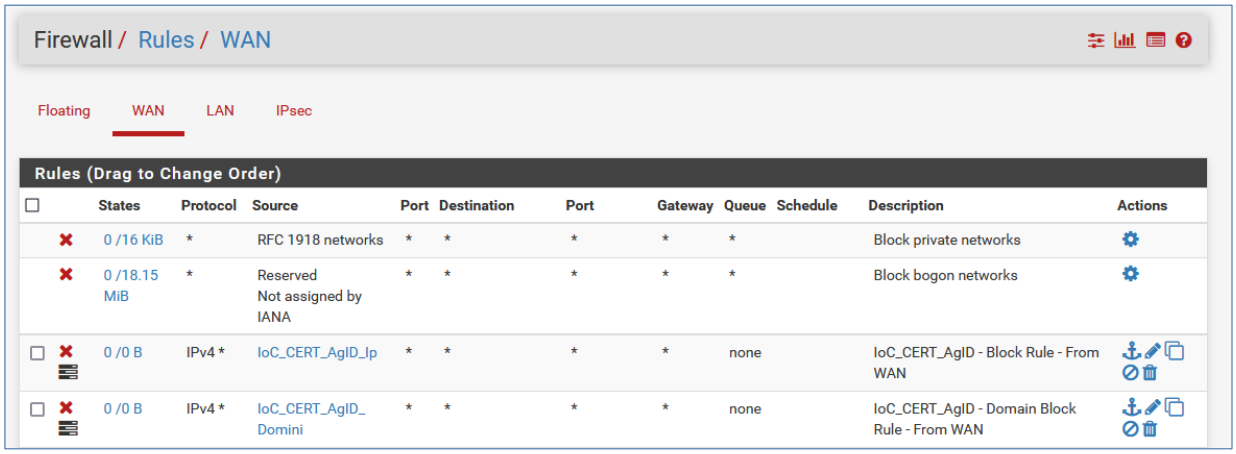
N.B.: dopo avere salvato le modifica confermare cliccando su **Apply changes**.



Creazione delle Rules

Interfaccia WAN

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

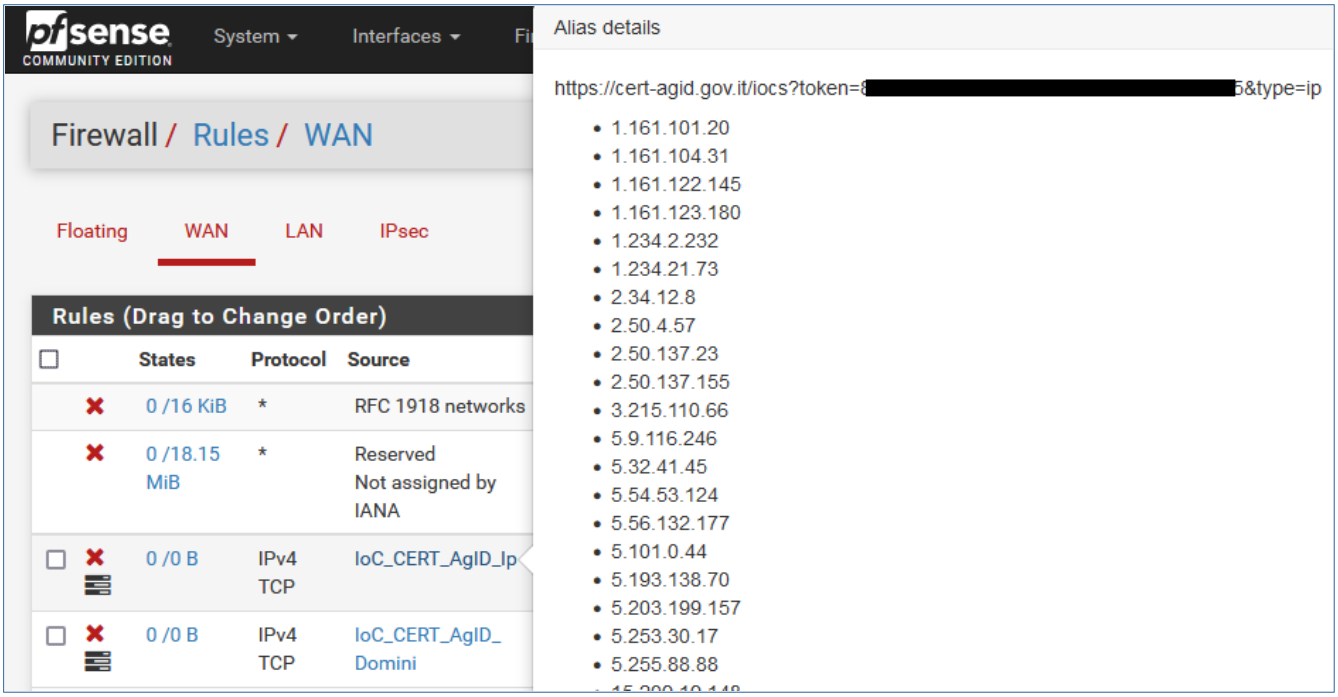
Action = Block;
Interface = LAN;
Address Family = IPv4;
Protocol = Any;
Source = Any;
Destination = "Single host or alias" -> "Nome Alias IP" [es. IoC_CERT_AgID_Ip]

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. IoC_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:



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.