UNIVERSIDAD DE GRANADA

CSIRC

Ciberseguridad: Técnicas de combate en Campus Universitarios Red HGP

Antonio Ruiz Moya

ARUIZ@UGR.ES

Servicio de Redes y Comunicaciones

Centro de Servicios de Informática y Redes de Comunicación

UNIVERSIDAD DE GRANADA

UNIVERSIDAD DE GRANADA

CSIRC

Anonimización del Tráfico de Red

Ejemplo:

Tor

Ultrasurf
PRIVACY. SECURITY. FREEDOM.

UNIVERSIDAD DE GRANADA
CSIRC

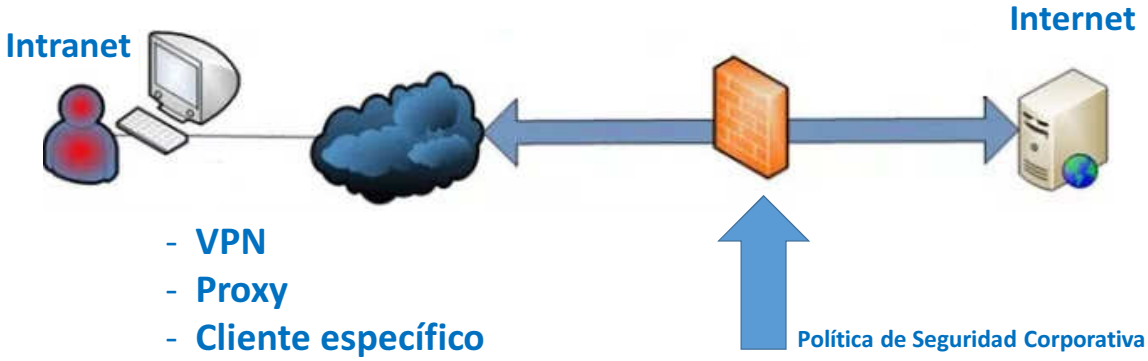
Legislación:

GDPR
ENS
Normativas internas
...

3

UNIVERSIDAD DE GRANADA
CSIRC

Métodos:

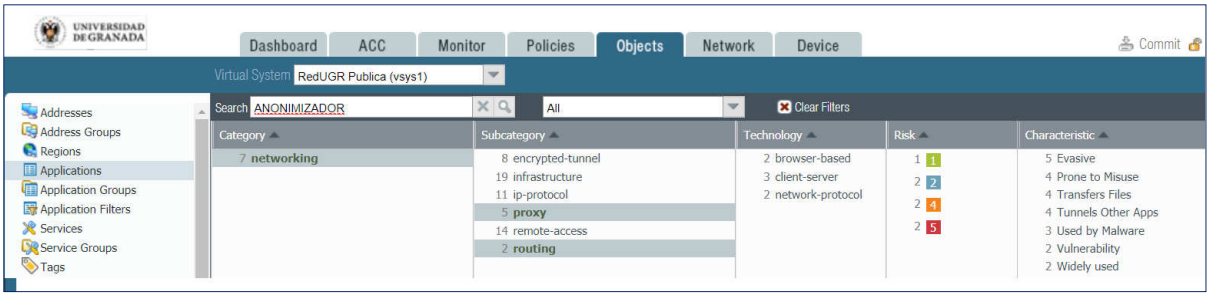


- **VPN**
- **Proxy**
- **Cliente específico**
- **...**

4

UNIVERSIDAD DE GRANADA
CSIRC

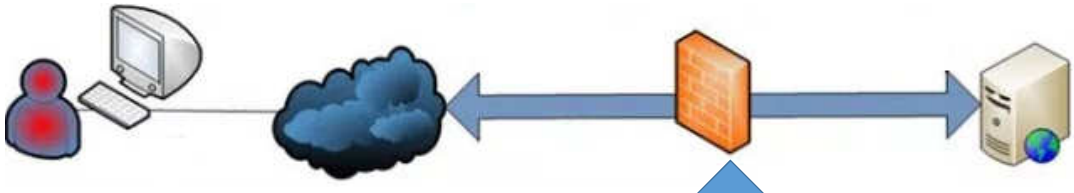
Evasión



5

UNIVERSIDAD DE GRANADA
CSIRC

Técnicas:



- **Puerto 53 (DNS)**
- **Puerto 25 (Correo)**
- **HTTP**
- **HTTPS**
- **UDP/TCP**
- **…**

Política de Seguridad Corporativa

6

UNIVERSIDAD DE GRANADA

CSIRC

Sistema HGP
HERMES Global Protection

Sistema de Sensores Servicios Ciberseguridad

Módulo de Detección de Anonimizadores de Red

Política de Seguridad Corporativa

7

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA

CSIRC

8

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection

>5.000 Anonimizadores públicos detectados

Metodologías Detección: Inteligentes y Dinámicas

Listas dinámicas de Filtrado en FW

9

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection
IMPLEMENTACION/Compatibilidad

paloalto networks
f5
FORTINET
Check Point

10

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection IMPLEMENTACION

You can enable Hermes Global Protection using External Dynamic List feature on Paloalto firewalls.

1. Create a new External Dynamic List (EDL) under **Objects > External Dynamic Lists > Add**
2. Complete the fields:
   - NAME: **Fighting Anonymizers** <Suggested name>
   - Type: **IP List** <List of IP addresses>
   - Description: **Source Anonymizer Servers by UGR** <Suggested description>
   - Source: **https://******** <URL provided by UGR>
   - Repeat: **Hourly** <Recommended refresh rate>
3. Use the new EDL **Fighting Anonymizers** on policy rules as you need (Eg: **Policies > Security > Add > Source > Source Address**)

paloalto NETWORKS

11

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection IMPLEMENTACION

You can enable Hermes Global Protection using IP Address Inteligence feature on F5 AFM firewalls.

1. Create a new Feed List under **Main Tab > Security > Network Firewall > IP Intelligence > Feed Lists > Create**
2. Complete the fields:
   - NAME: **Fighting Anonymizers** <Suggested name>
   - Feed:
     - URL: **https://******** <URL provided by UGR>
     - List Type: **Blacklist**
     - Blacklist Category: **Proxy/Anonymous Proxies** <Suggested category>

f5

12

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection IMPLEMENTACION

You can enable Hermes Global Protection using Threat Feed Connectors feature on Fortinet firewalls.

1. Create a new Threat Feed under **Security Fabric > Fabric Connectors**
2. Complete the fields:
   - NAME: **Fighting Anonymizers** <Suggested name>
   - Category: **IP Address** <List of IP addresses>
   - URI of external resource: **https://******** <URI provided by UGR>
   - HTTP basic authentication: **disabled** <Authentication not needed>
   - Refresh Rate: **60** <Recommended refresh rate>
3. The feed **Fighting Anonymizers** will appear as an "External IP Block List" in DNS Filter profiles and as a "Source/Destination" in IPv4, IPv6, and Proxy policies.

FORTINET

13

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection IMPLEMENTACION

You can enable Hermes Global Protection using Custom IP Feeds feature on Checkpoint firewalls from Management Server.

1. Create a plain text file containing your Security Gateways (one name or IP each line)
2. Create a plain text file containing the URL **https://******<URL provided by UGR>
3. Activate the feature following this tutorial.

Check Point

14

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection
¿Cómo Incorporarse en HGP?

MODALIDADES DE USO:
HGP-CC: CLIENTE CONSUMIDOR
HGP-CP: CLIENTE PRODUCTOR

15

UNIVERSIDAD DE GRANADA
CSIRC

HGP: HERMES Global Protection
¿Cómo Incorporarse en Red HGP?

HGP-CC: NOC@UGR.ES

- Compromiso
- Interlocutor/mail
- IP del Consumidor
- Modelo de FW

16

UNIVERSIDAD DE GRANADA

CSIRC

HGP: HERMES Global Protection
¿Cómo Incorporarse en Red HGP?

HGP-CP: NOC@UGR.ES

- Compromiso, Interlocutor/mail, IP del Consumidor y Modelo de FW
- Nodo Windows 7/8/10 English versión, RDP o similar, Acceso al Sistema HGP activo en FW

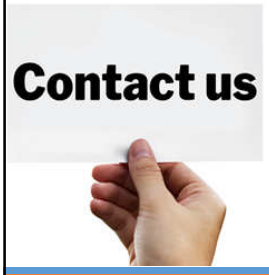
17

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA

CSIRC

HGP: HERMES Global Protection
Más información:



NOC@UGR.ES

18

Jornadas Técnicas de RedIRIS 2019, Sevilla 28-30 de Mayo de 2019 Ciberseguridad: técnicas de combate en campus universitarios. Red HGP

UNIVERSIDAD DE GRANADA

CSIRC

Ciberseguridad:
Técnicas de combate en Campus Universitarios
Red HGP

ANTONIO RUIZ MOYA

ARUIZ@UGR.ES

SERVICIO DE REDES Y COMUNICACIONES

UNIVERSIDAD DE GRANADA

Rectorado de la Universidad de Sevilla (Real Fábrica de Tabacos)