FHRP Nightmare

Magama Bazarov

Network Security Expert

Moscow, August 25, 2022

Who I am

Network Security Expert, Network Engineer

- Alias: @in9uz
- Author of articles on “Xakep” magazine
- Author of “Nightmare” style articles

Agenda

- What is FHRP?
- FHRP Theory (HSRP, VRRP, GLBP)
- Hijacking Process Theory
- Vectors & Problems
- HSRP Hijacking
- VRRP Hijacking
- GLBP Hijacking
- Prevention

What is FHRP?

FHRP (First Hop Redundancy Protocol)

Is a family of protocols that allow for redundancy of the default network gateway. The general idea of using FHRP protocols is to combine several physical routers into one logical router with a common IP address. This IP address of the virtual router will be assigned on the hosts as the default gateway address.

HSRP Theory. Part I

HSRP (Hot Standby Router Protocol)

- Cisco proprietary
- HSRPv1 & HSRPv2
- RFC 2281
- UDP/1985 (over TCP/IP)
- 224.0.0.2 & 224.0.0.102

HSRP Theory. Part II

Entities & Terminology

- Active Router
- Standby Router
- HSRP Group
- HSRP MAC (00:00:0C:07:AC:XX) (XX – this is a HSRP Group Number)
- HSRP Virtual IP Address

VRRP Theory. Part I

VRRP (Virtual Router Redundancy Protocol)

- HSRP-based
- RFC 5798
- Supported by all vendors of network equipment
- L3 Protocol
- 224.0.0.18

VRRP Theory. Part II

Entities & Terminology

- Master Router
- Backup Router
- VRRP Group (VRID)
- VRRP MAC (00:00:5E:01:XX) (XX – this is a VRRP group number)
- VRRP Virtual IP Address

GLBP Theory. Part I

GLBP (Gateway Load Balancing Protocol)

- Cisco proprietary
- RFC is not available.
- Real load balancing
- UDP/3222 (over TCP/IP stack)
- 224.0.0.102

GLBP Theory. Part II

Entities & Terminology

- AVG Router
- AVF Router
- GLBP Group
- GLBP MAC (00:07:B4:00:XX:YY) (XX – GLBP Group Number) (YY – GLBP AVF Number)
- GLBP Virtual IP Address
- GLBP Weight Metric

FHRP Timings

- HSRP (Hello time: 3 sec, Hold time: 10 sec)
- VRRP (Hello time: 1 sec, Hold time: 3 sec)
- GLBP (Hello time: 3 sec, Hold time: 10 sec)

FHRP Selector

- The device with the largest address will become a master router (by default)
- The priority value is set manually. Highest value wins
- Preempt mode. (Disabled by default in HSRP & GLBP)

Vectors

- MITM
- Blackhole Attack
- Kicking the router via UDP Flood (HSRP, UDP/1985 & GLBP, UDP/3222)

Limitations

- Dependence on network segmentation
- Requires powerful hardware
- Performance network interface

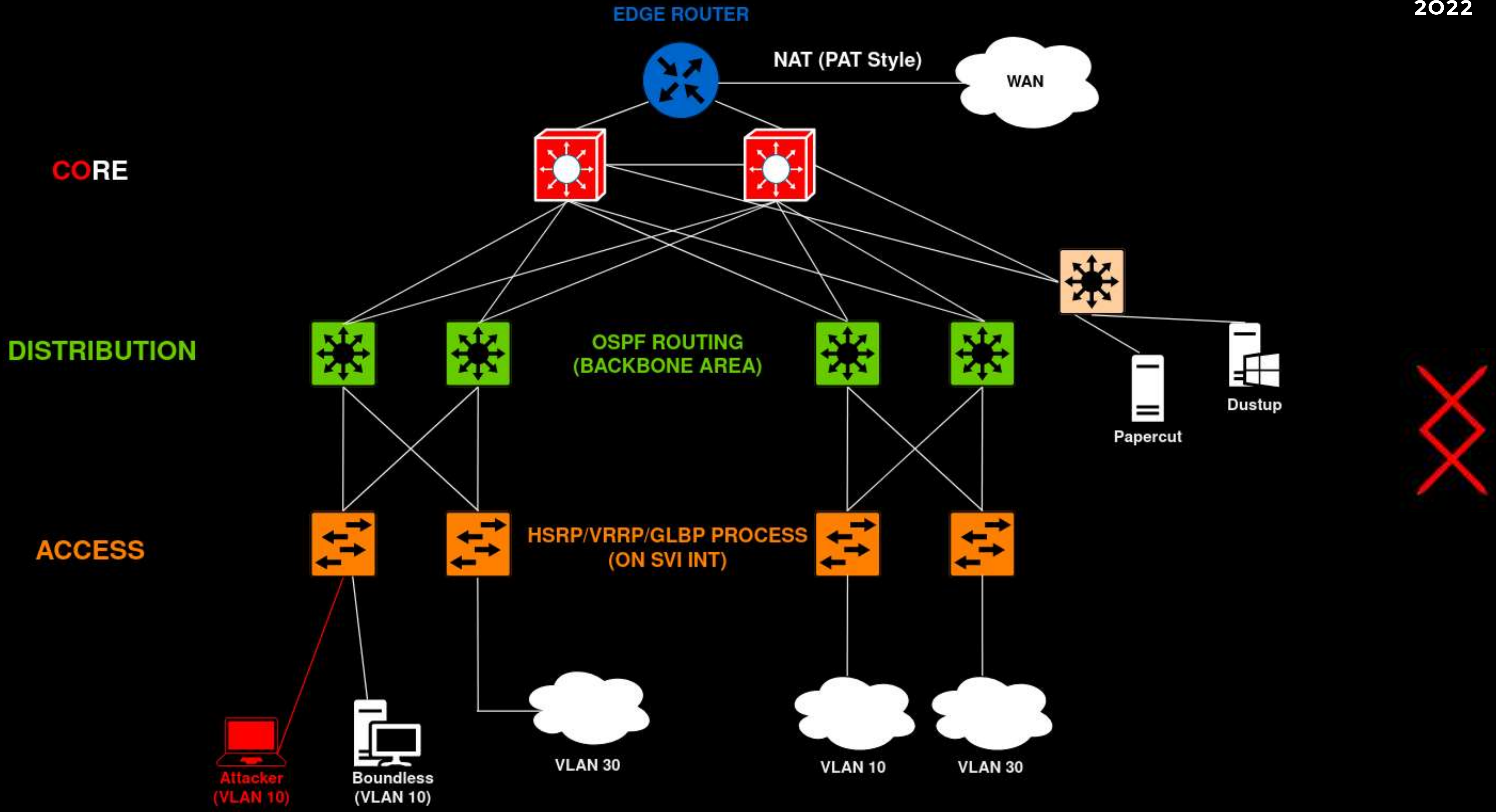
Weaponize

- Wireshark
- John & *2john exfiltrators
- Loki

Hijacking Theory

- Information Gathering
- Checking for cryptographic authentication (a bruteforce attack is possible)
- Sending a malicious FHRP injection (priority 255, weight value 255)
- Creating a secondary address, routing management, configuring the NAT mechanism

Nightmare Realm



HSRP Demo

VRRP Demo

GLBP Demo

Prevention

1. ACL against HSRP traffic (224.0.0.2 / 224.0.0.102, UDP/1985)
2. ACL against VRRP traffic (224.0.0.18)
3. ACL against GLBP traffic (224.0.0.102, UDP/3222)
4. Cryptographic authentication
5. Highest priority value (for HSRP & GLBP)

The nightmare is over.