IPv6

IPv6 is the latest version of Internet Protocol, overcoming IPv4 limitations by utilizing 128-bit addresses to accommodate the increasing number of connected devices. It offers enhanced performance and security with features like simplified packet headers, quality of service support, and mandatory IPsec encryption. IPv6 allows for virtually limitless device connections and facilitates direct addressing, ensuring the internet's continued growth and evolution.

IPv6

Unicast addresses in IPv6 facilitate one-to-one communication by identifying a single device interface, supporting vast unique addresses with its 128-bit scheme.

Multicast addresses enable one packet to be sent to multiple destinations simultaneously, reducing network traffic for applications like streaming media.

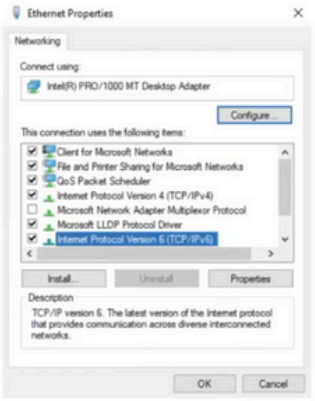
Anycast addresses, assigned to multiple interfaces across devices, direct packets to the nearest interface, optimizing load balancing and improving network resilience.

IPv6

SLAAC

Stateless Address Autoconfiguration is a method used by IPv6 for automatic assignment of IP addresses without the need for a server like DHCP. When a device is connected to an IPv6 network using SLAAC, it listens for router advertisements that include a prefix for the network. The device then generates its own IP address by combining this prefix with a unique identifier generated from its own hardware, often the MAC address.

Dual Stack



Zero Trust

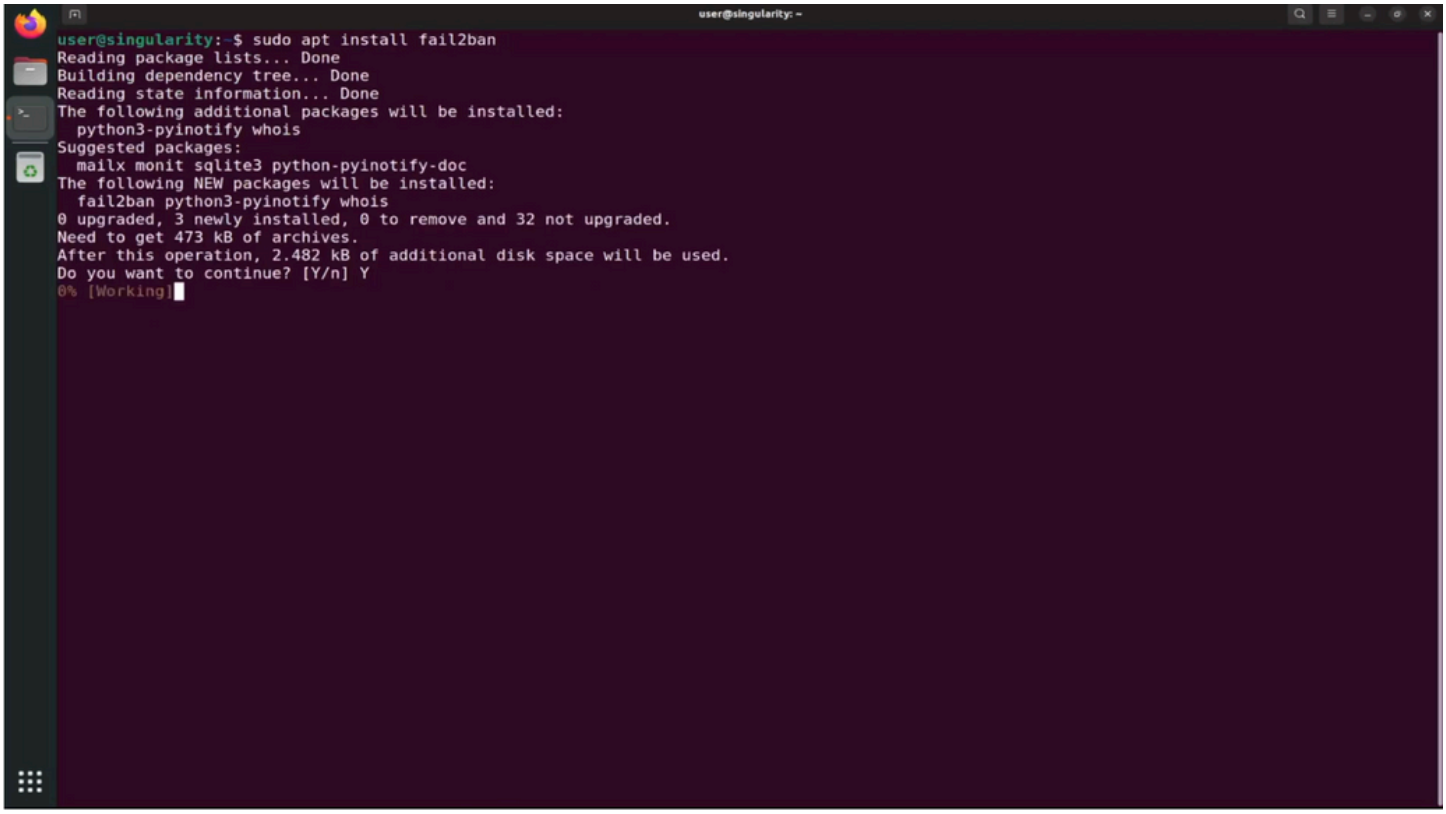
Zero Trust is a security concept that operates on the principle of never trusting, always verifying. In a Zero Trust model, no entity, whether inside or outside the network perimeter, is automatically trusted. Instead, all users, devices, and applications must be authenticated and authorized before accessing resources.

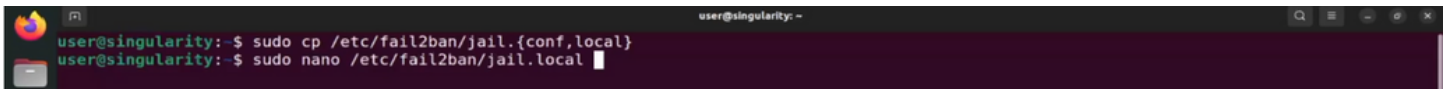
This approach assumes that threats could be present both inside and outside the network and emphasizes continuous monitoring and strict access controls to prevent unauthorized access and mitigate potential breaches. By adopting Zero Trust principles, organizations aim to enhance their security posture and protect sensitive data and assets effectively.

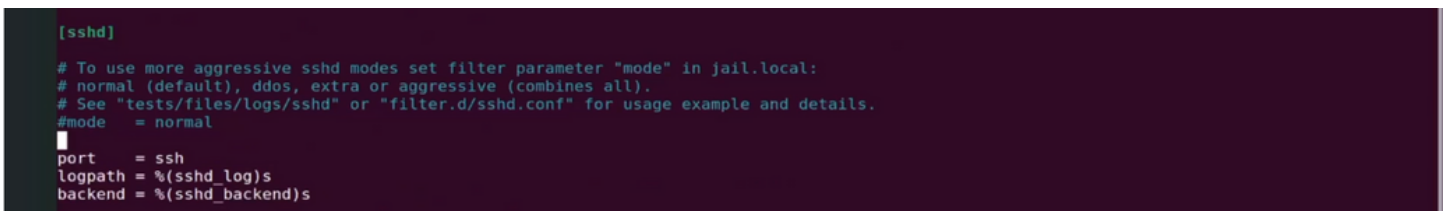
Zero Trust

Example: In the case **of internal threats (insiders),** whether from employees or an attacker who has gained access, Zero Trust employs these three techniques to mitigate the attack:

- **Microsegmentation**: Adds granularity to the design by creating small security perimeters that isolate the attacker, using methods like authentication and authorization, for instance.
- **User Identification**: Zero Trust treats all users as untrustworthy, so if anyone attempts to perform a suspicious task, they will be monitored at all times.
- **Access Control**: The principle of applying the least privileges possible is also used in Zero Trust. Therefore, higher access privileges are only granted when absolutely necessary.







```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
enabled = true
port    = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 600
backend = %(sshd_backend)s
```

```
user@singularity:~$ sudo systemctl restart fail2ban
user@singularity:~$
```

```
user@singularity:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
user@singularity:~$
```

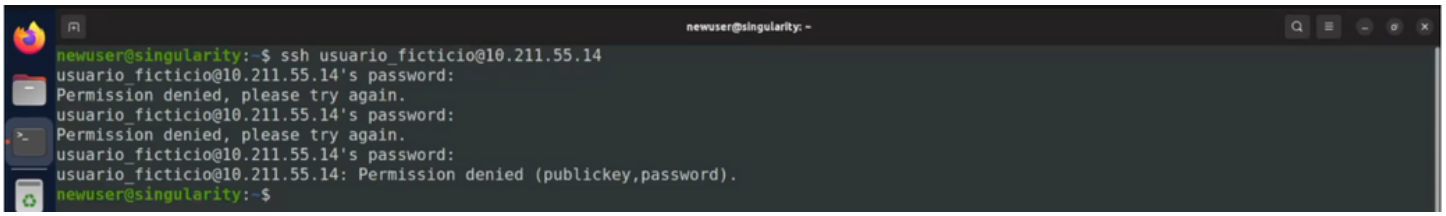
```
user@singularity:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:1c:42:f4:42:b0 brd ff:ff:ff:ff:ff:ff
    inet 10.211.55.14/24 brd 10.211.55.255 scope global dynamic noprefixroute enp0s5
       valid_lft 1478sec preferred_lft 1478sec
    inet6 fdb2:2c26:f4e4:0:de39:af0b:12d6:20b3/64 scope global temporary dynamic
       valid_lft 590081sec preferred_lft 71453sec
    inet6 fdb2:2c26:f4e4:0:7be9:e6bb:94d6:4b43/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591942sec preferred_lft 604742sec
    inet6 fe80::9e29:c195:bc7e:7155/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
user@singularity:~$
```

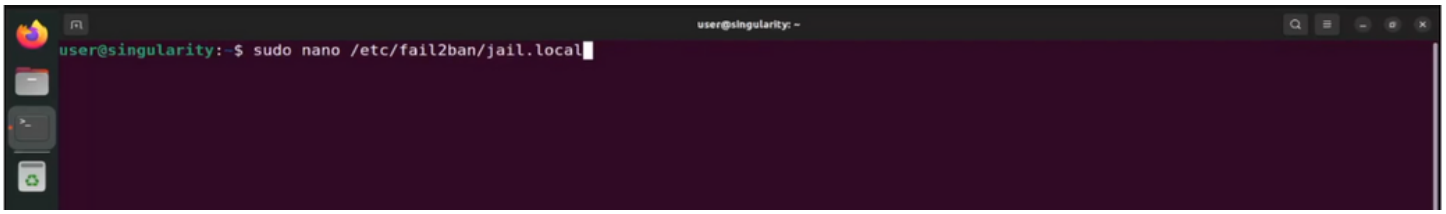
newuser@singularity: ~

```
newuser@singularity:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:1c:42:cd:3c:60 brd ff:ff:ff:ff:ff:ff
    inet 10.211.55.15/24 brd 10.211.55.255 scope global dynamic noprefixroute enp0s5
       valid_lft 1286sec preferred_lft 1286sec
    inet6 fdb2:2c26:f4e4:0:5beb:314:8db:e1b7/64 scope global temporary dynamic
       valid_lft 590788sec preferred_lft 72117sec
    inet6 fdb2:2c26:f4e4:0:b80f:ecab:6061:1c2e/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591747sec preferred_lft 604547sec
    inet6 fe80::dcec:2c02:2985:f571/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
newuser@singularity:~$
```

newuser@singularity: ~

```
newuser@singularity:~$ ping 10.211.55.14
PING 10.211.55.14 (10.211.55.14) 56(84) bytes of data.
64 bytes from 10.211.55.14: icmp_seq=1 ttl=64 time=0.377 ms
64 bytes from 10.211.55.14: icmp_seq=2 ttl=64 time=0.534 ms
```


newuser@singularity: ~
newuser@singularity:~$ ssh usuario_ficticio@10.211.55.14
usuario_ficticio@10.211.55.14's password:
Permission denied, please try again.
usuario_ficticio@10.211.55.14's password:
Permission denied, please try again.
usuario_ficticio@10.211.55.14's password:
usuario_ficticio@10.211.55.14: Permission denied (publickey,password).
newuser@singularity:~$


user@singularity: ~
user@singularity:~$ sudo nano /etc/fail2ban/jail.local

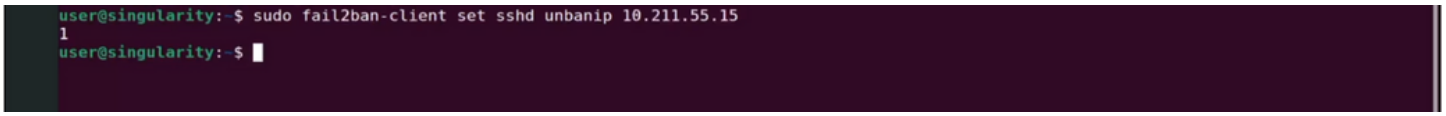

[sshd]
To use more aggressive sshd modes set filter parameter "mode" in jail.local:
normal (default), ddos, extra or aggressive (combines all).
See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
enabled = true
port   = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
backend = %(sshd_backend)s


user@singularity:~$ sudo systemctl restart fail2ban
user@singularity:~$ c

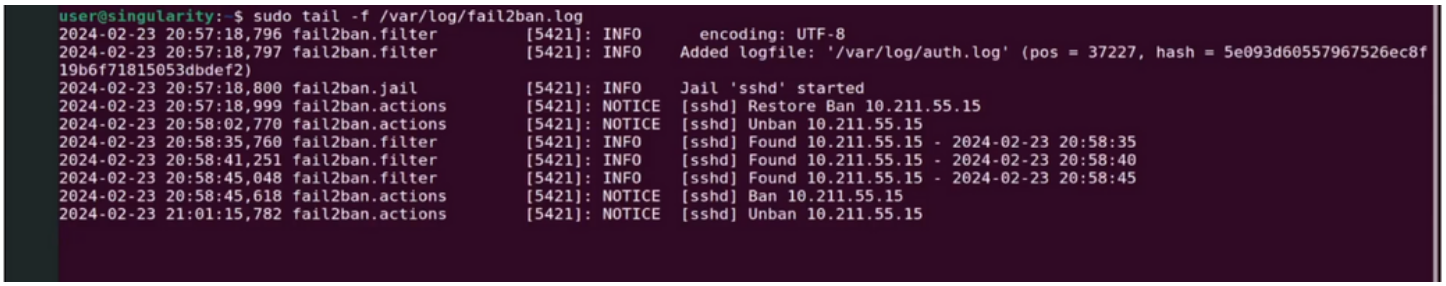

user@singularity: ~
user@singularity:~$ sudo fail2ban-client status
Status
|- Number of jail: 1
`- Jail list: sshd
user@singularity:~$


newuser@singularity:~$ ssh usuario_ficticio@10.211.55.14
usuario_ficticio@10.211.55.14's password:
Permission denied, please try again.
usuario_ficticio@10.211.55.14's password:
Permission denied, please try again.
usuario_ficticio@10.211.55.14's password:


user@singularity: ~
user@singularity:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 3
| `- File list: /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `- Banned IP list: 10.211.55.15
user@singularity:~$


user@singularity:~$ sudo fail2ban-client set sshd unbanip 10.211.55.15
1
user@singularity:~$


user@singularity:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 3
| `- File list: /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned: 1
   `- Banned IP list:
user@singularity:~$



Conclusion

IPv6 enhances network security with features like built-in IPsec and simplified packet headers, but implementing a Zero Trust approach is crucial for comprehensive data security. Zero Trust principles ensure continuous verification and strict access controls, mitigating potential threats and safeguarding network resources effectively.