Network Analysis: pfSense®

Joe Abraham
CYBERSECURITY CONSULTANT

@joeabrah www.defendthenet.com


pfsense®

Creators: Chris Buechler and Scott Ullrich

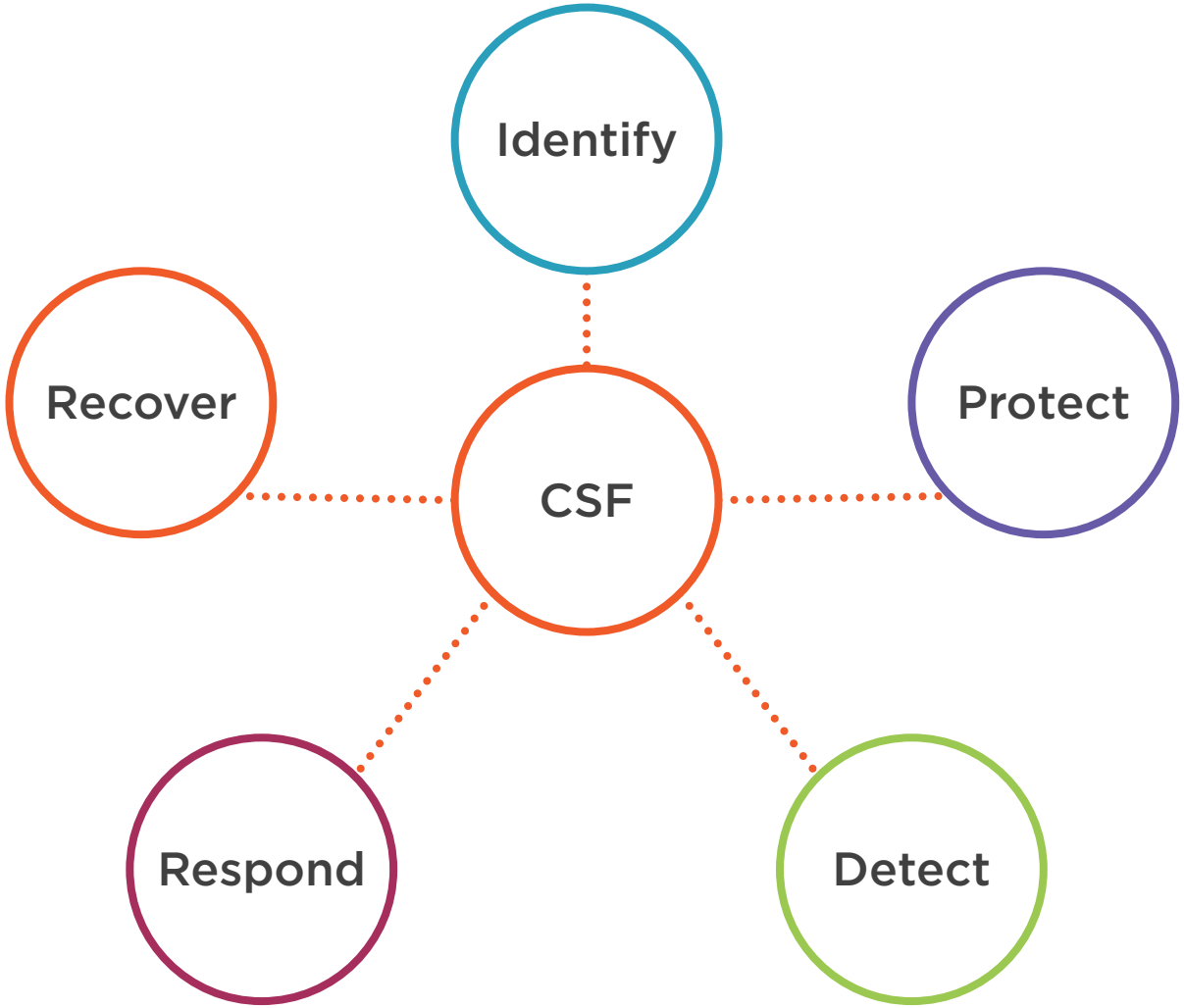
The pfSense project is a free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third party free software packages for additional functionality. pfSense software, with the help of the package system, is able to provide the same functionality or more of common commercial firewalls, without any of the artificial limitations.

pfSense is a free firewall distribution with a web interface, requiring no UNIX or command line knowledge.

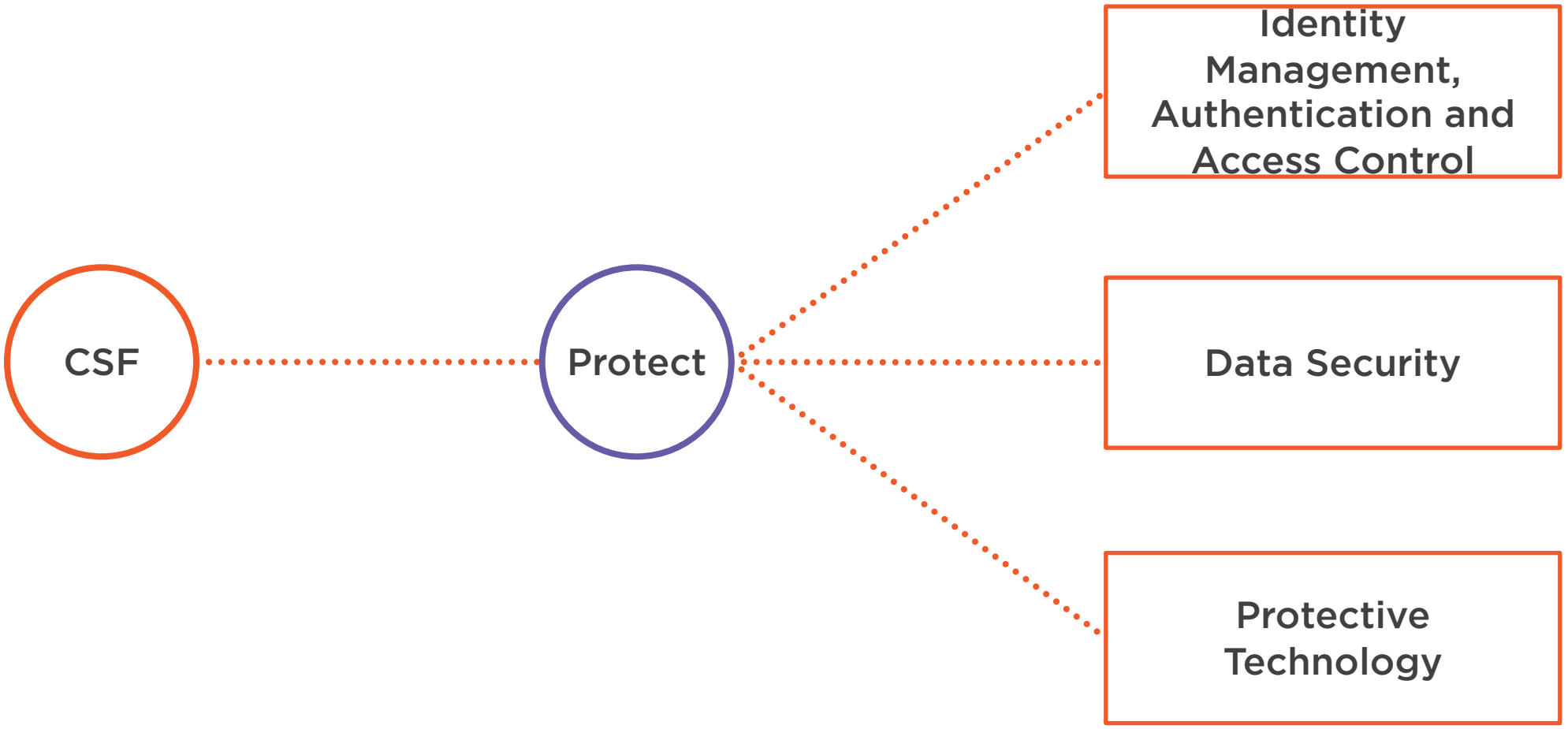
It can be downloaded at https://www.pfsense.org/download/

Pfsense provides a package system that adds functionality to the firewall distribution. These packages expand the functionality from traditional IP and port blocking to VPN, DNS blocking, DHCP, proxy, network monitoring, and IPS capabilities

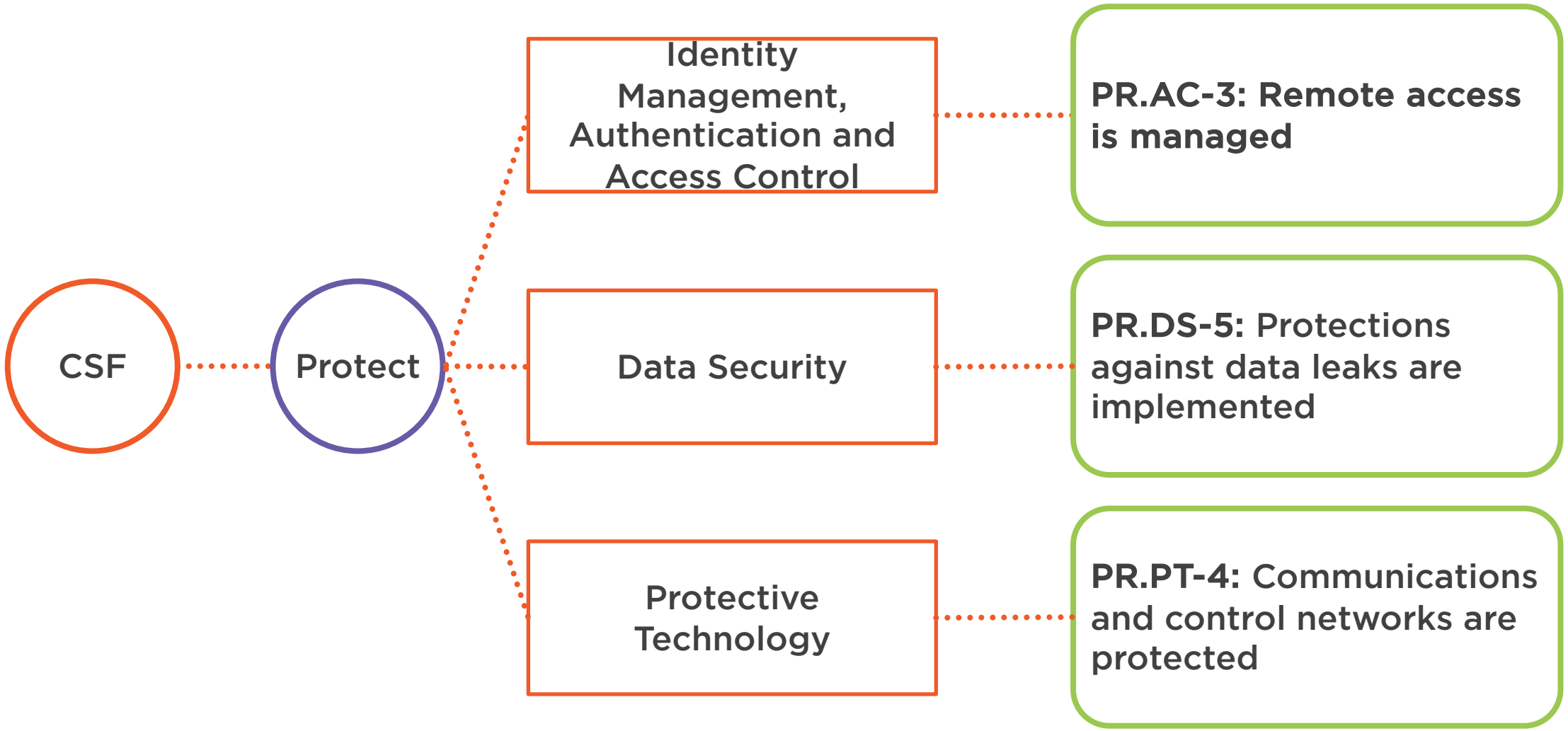
NIST Cybersecurity Framework



NIST Cybersecurity Framework



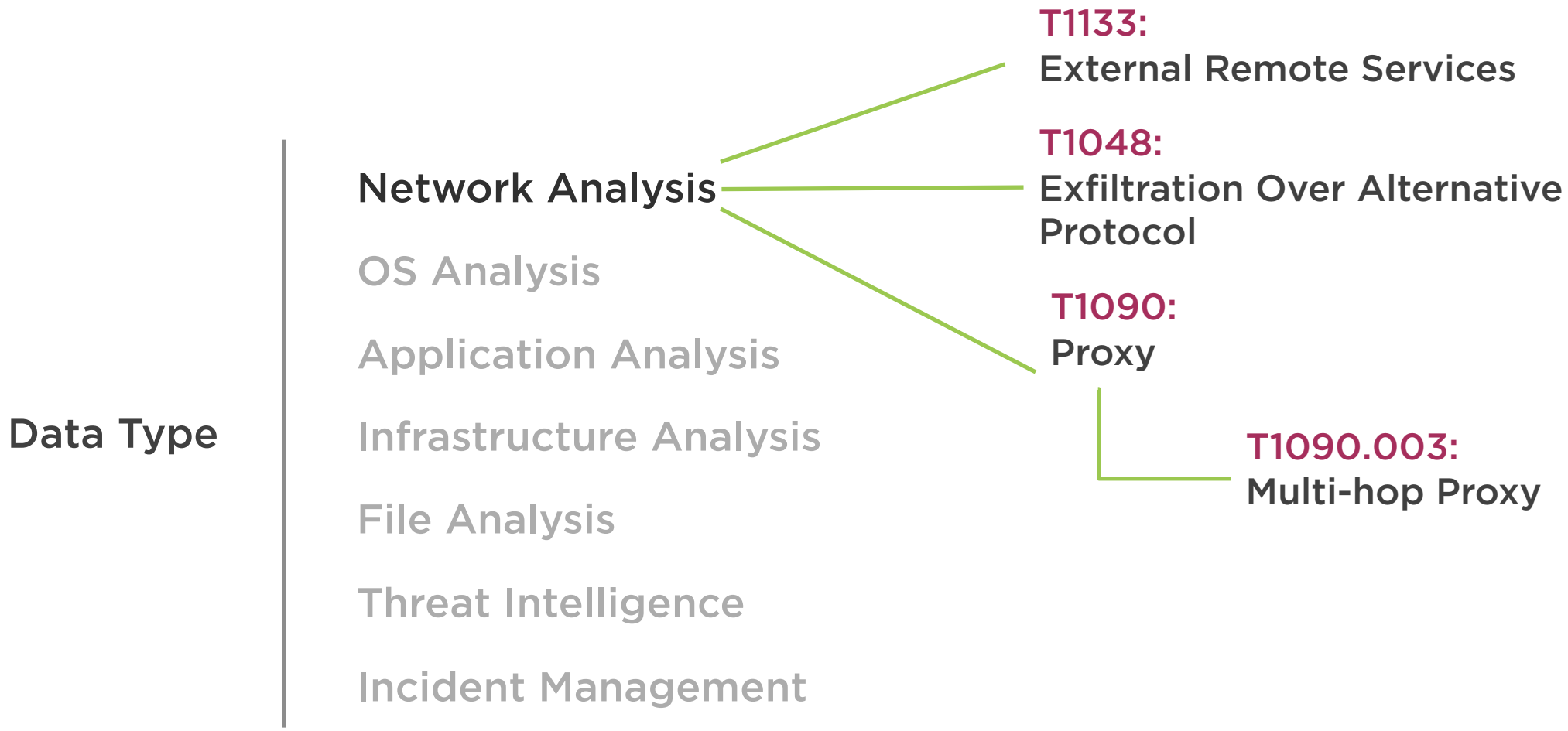
NIST Cybersecurity Framework



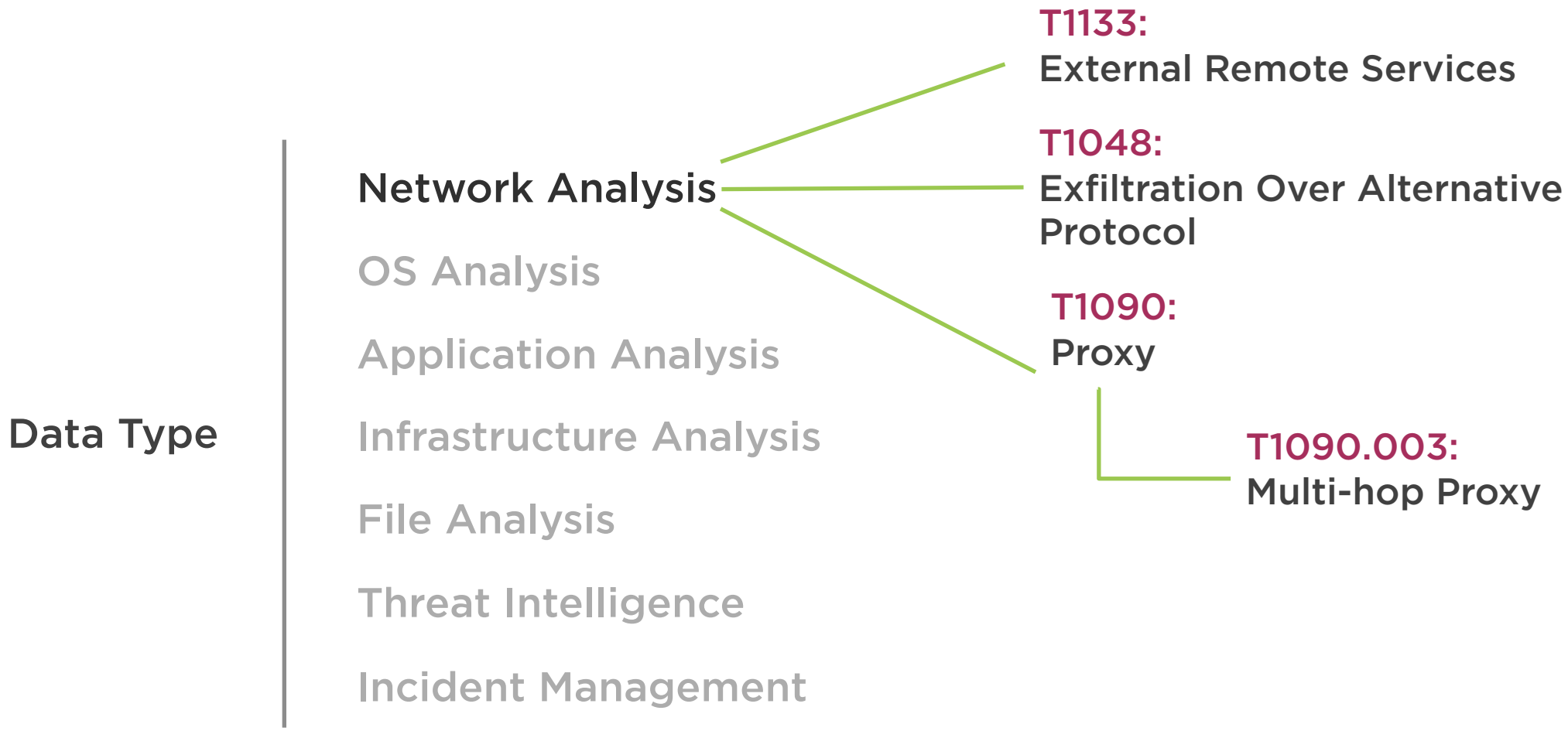
MITRE ATT&CK

Data Analysis Type	Network Analysis
	OS Analysis
	Application Analysis
	Infrastructure Analysis
	File Analysis
	Threat Intelligence
	Incident Management

MITRE ATT&CK


Data Type
Network Analysis
OS Analysis
Application Analysis
Infrastructure Analysis
File Analysis
Threat Intelligence
Incident Management
T1133:
External Remote Services
T1048:
Exfiltration Over Alternative Protocol
T1090:
Proxy
T1090.003:
Multi-hop Proxy

MITRE ATT&CK


Data Type
Network Analysis
OS Analysis
Application Analysis
Infrastructure Analysis
File Analysis
Threat Intelligence
Incident Management
T1133:
External Remote Services
T1048:
Exfiltration Over Alternative Protocol
T1090:
Proxy
T1090.003:
Multi-hop Proxy

MITRE SHIELD

T1133:
External Remote Services

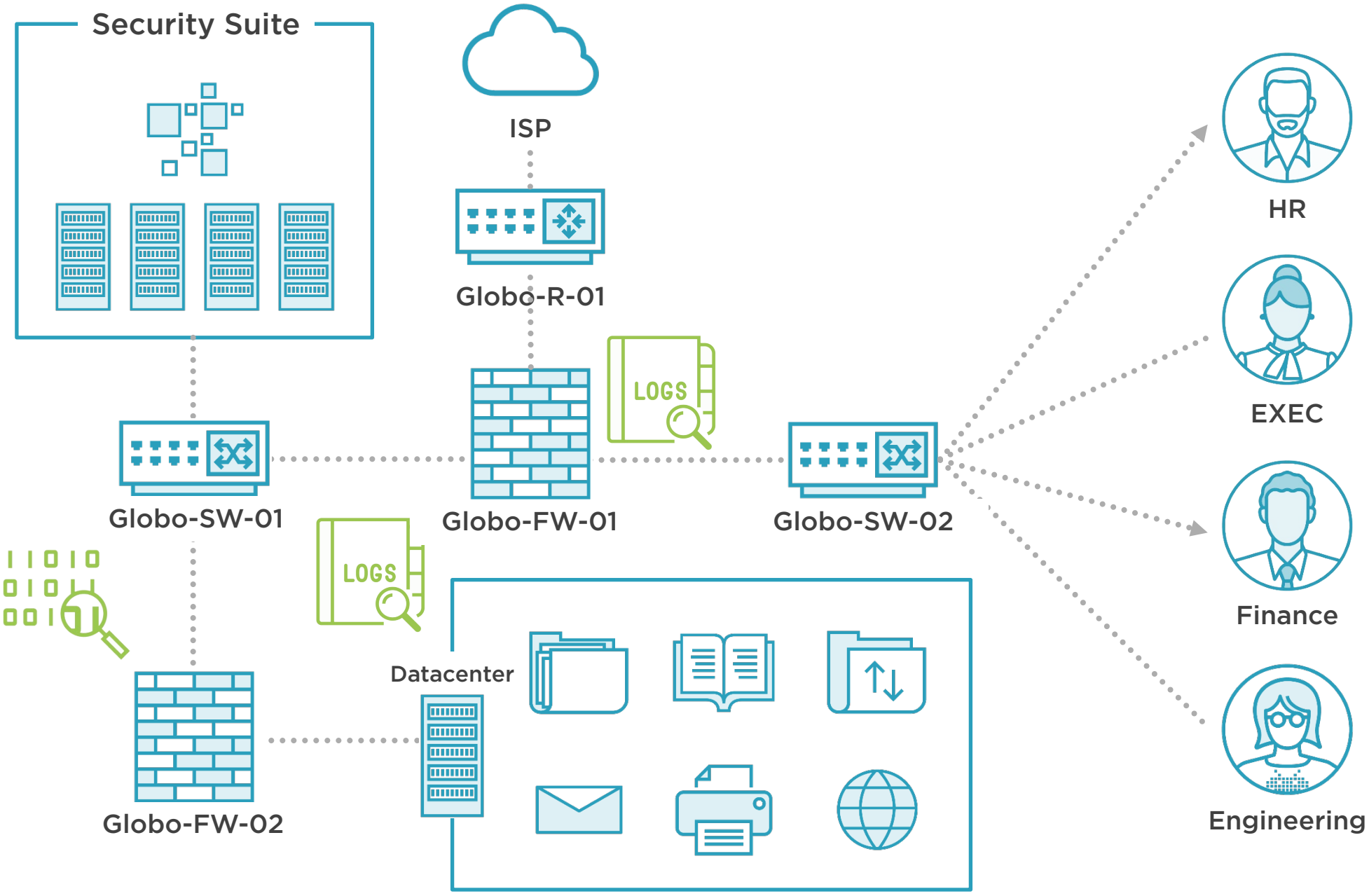
DTE0017 – Decoy System: A defender can setup a decoy VPN server and see if an adversary attempts to use valid account to authenticate it. (DUC0009)

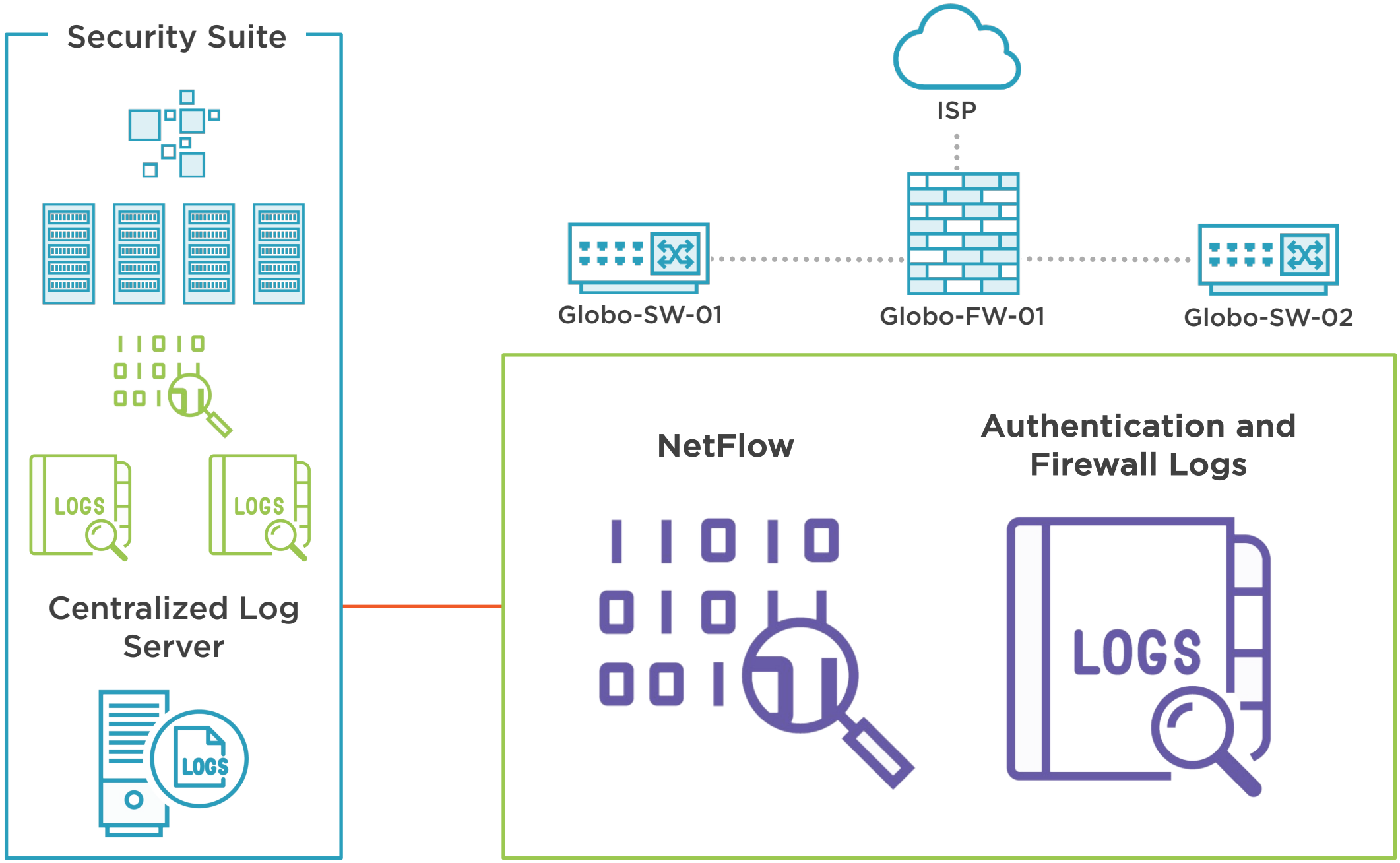
T1048:
Exfiltration Over
Alternative Protocol

DTE0026 – Network Manipulation: A defender can prevent or enable use of alternate protocols for exfiltration by blocking/unblocking unnecessary ports and protocols. (DUC0174)

T1090.003:
Multi-hop Proxy

DTE0026 – Network Manipulation: A defender could block traffic to known anonymity networks and C2 infrastructure through the use of network allow and block lists. (DUC0164)


Security Suite
ISP
Globo-R-01
LOGS
Globo-SW-01
Globo-FW-01
Globo-SW-02
HR
EXEC
Finance
Engineering
LOGS
Datacenter
Globo-FW-02


Security Suite
LOGS
LOGS
Centralized Log Server
LOGS
ISP
Globo-SW-01
Globo-FW-01
Globo-SW-02
NetFlow
Authentication and Firewall Logs
LOGS

More Information

Capabilities

Using NAT with pfSense

https://docs.netgate.com/pfsense/en/latest/recipes/ftp-without-proxy.html

Configuring a Transparent Proxy

https://docs.netgate.com/pfsense/en/latest/recipes/http-client-proxy-transparent.html

Additional pfSense information

https://www.pfsense.org/get-involved/

Related Information

MITRE Shield Tactics and Information

https://shield.mitre.org/tactics/DTA0004/

Supporting Information

- pfBlocker-NG Package: https://pfsense-docs.readthedocs.io/en/latest/packages/pfblocker.html
- OpenVPN: https://openvpn.net