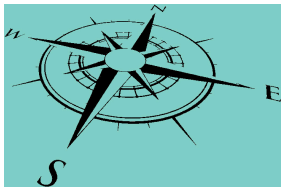
Trusted Internet Connections 3.0 -- Vol. 3: Policy Enforcement Point Capabilities

Policy Enforcement Point (PEP) Capabilities are network-level capabilities that inform technical implementation for relevant use cases. PEP Capabilities are divided into eight groups and fulfilled by applications, devices, or services identified in TIC Use Cases and TIC Overlays. The eight PEP capability groups correspond to the following security functions:

- Files,
- Email,
- Web,
- Networking,
- Resiliency,
- DNS,
- Intrusion Detection, and
- Enterprise.

The PEP capability groups listing is not exhaustive. Additional groups may be developed to reflect new use cases. The following tables provide: (1) a list of PEP capabilities, (2) a description of each capability, and (3) a mapping to relevant NIST CSF categories.

Contents



Cybersecurity and Infrastructure Security Agency (CISA)

Description:

Cybersecurity Division

Mission

To inform technical implementation of network-level capabilities

1. Files

Secure files

Files PEP Security Capabilities

1.1. Malware

Detect the presence of malicious code and facilitate its quarantine or removal

Anti-Malware — Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.

1.2. Disarming & Reconstruction

Detect the presence of unapproved active content and facilitates its removal

Content Disarm & Reconstruction — Content Disarm & Reconstruction technology detects the presence of unapproved active content and facilitates its removal.

1.3. Detonation

Facilitate the detection of malicious code through the use of protected and isolated execution environments

Detonation Chambers — Detonation Chambers facilitate the detection of malicious code through the use of protected and isolated execution environments to analyze the files

2. E-Mail

Secure E-mail

Email PEP Security Capabilities

2.1. Phishing

Detect instances of phishing and prevent users from accessing them

Anti-phishing Protections — Anti-phishing protections detect instances of phishing and prevent users from accessing them.

2.2. SPAM

Detect and quarantine SPAM

Anti-SPAM Protections — Anti-SPAM protections detect and quarantine instances of SPAM.

2.3. Authentication

Allow downstream entities to accept an intermediary's authentication even if the email was changed

Authenticated Received Chain — Authenticated Received Chain allows for an intermediary, like a mailing list or forwarding service, to sign its own authentication of the original email, allowing downstream entities to accept the intermediary's authentication even if the email was changed.

2.4. Loss

Detect exfiltration of data

Data Loss Prevention — Data Loss Prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data

2.5. Incoming

Authenticate incoming email

DMARC for Incoming Email — DMARC protections authenticate incoming email according to the DMARC email authentication protocol defined in RFC 7489.

2.6. Outgoing

Sign emails

DMARC for Outgoing Email — DMARC protections facilitate the authentication of outgoing email by signing the emails and ensuring that external parties may validate the email signatures. The DMARC email authentication protocol is defined in RFC4789.

2.7. Encryption

Configured email services to use encrypted connections

Encryption for Email Transmission — Email Services are configured to use encrypted connections, when possible, when interacting with Clients and other Email Servers.

2.8. URLs

Detect malicious URLs in emails and prevent users from accessing them

Malicious URL Protections — Malicious URL Protections detect malicious URLs in emails and prevent users from accessing them.

2.9. Click-Throughs

Verify the security of URL destinations before permitting access

URL Click-Through Protection — URL Click-Through Protections ensures that when a URL from an email is clicked, the requester is directed to a protection that verifies the security of the URL destination before permitting access.

2.10. Intrusions

Prevent intrusions

NCPS E3A Protections — NCPS E3A is an intrusion prevention capability, provided by DHS, that includes an Email Filtering security service.

3. Web

Secure Web access

Web PEP Security Capabilities

3.1. Break & Inspect

Terminate encrypted traffic, inspect, and re-encrypt it

Break and Inspect — Break-and-Inspect systems terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re-encrypting the traffic, if applicable, before transmitting to the final destination.

3.2. Active Content

Detect and facilitate removal of unapproved active content

Active Content Mitigation — Active Content Mitigation protections detect the presence of unapproved active content and facilitate its removal.

3.3. Blacklisting

Prevent communication with entities using bad certificates

Certificate Blacklisting — Certificate Blacklisting protections prevent communication with entities that use a set of known bad certificates.

3.4. Certificates

Prevent use of inconsistent credentials

Certificate Consensus — Certificate Consensus provides a comparison of all observed certificates in use for consistency and preventing use of inconsistent credentials.

3.5. Unapproved Content

Detect and facilitate removal of unapproved content

Content Filtering — Content Filtering protections detect the presence of unapproved content and facilitate its removal.

3.6. Authentication

Require entities to authenticate with the proxy

Authenticated Proxy — Authenticated Proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.

3.7. Data Loss

Detect instances of the exfiltration

Data Loss Prevention — Data Loss Prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.

3.8. DNS-over-HTTPS

Prevent usage of the DNS-over-HTTPS protocol

DNS-over-HTTPS — Filtering DNS-over-HTTPS filtering prevents entities from using the DNS-over-HTTPS protocol, possibly evading DNS-based protections.

3.9. Enforcement

Ensure that traffic complies with protocol definitions

RFC Compliance Enforcement — RFC Compliant Enforcement technologies ensure that traffic complies with protocol definitions.

3.10. Filtering

[Establish] different security protections for classes of domains

Domain Category Filtering — Domain Category Filtering technologies allow for classes of domains (e.g. banking, medical) to receive a different set of security protections.

3.11. Reputation

Blacklist domains based on reputation

Domain Reputation Filter — Domain Reputation Filtering protections are a form of Domain Blacklisting based on a domain's reputation, as defined by either the agency or an external entity.

3.12. Bandwidth

Limit the amount of bandwidth used by different classes of domains

Bandwidth Control — Bandwidth Control technologies allow for limiting the amount of bandwidth used by different classes of domains.

3.13. Filtering

Detect and facilitate removal of malicious content

Malicious Content Filtering — Malicious Content Filtering protections detect the presence of malicious content and facilitate its removal.

3.14. Access

Define policies concerning what entities may perform

Access Control — Access Control technologies allow an agency to define policies concerning what entities may perform.

4. Networks

Secure networks

Networking PEP Security Capabilities

4.1. Access

Prevent the ingest or transiting of unauthorized network traffic

Network Access Controls — Network Access Control protections prevent the ingest or transiting of unauthorized network traffic.

4.2. Blacklisting

Prevent the ingest or transiting of traffic received from or destined to a blacklisted IP address

IP Blacklisting — IP Blacklisting protections prevent the ingest or transiting of traffic received from or destined to a blacklisted IP address.

4.3. Containment

Enable revocation of hosts' access to networks

Host Containment — Host Containment protections enable a network to revoke a host's access to the network.

4.4. Segmentation

Separate networks into subnetworks

Network Segmentation — Network Segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.

4.5. Microsegmentation

Divide networks according to the communication needs of application and data workflows

Microsegmentation — Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.

5. Resiliency

Resiliency PEP Security Capabilities

5.1. DDoS

Mitigate the effects of distributed denial of service attacks

DDoS Protections — DDoS protections mitigate the effects of distributed denial of service attacks.

5.2. Expansion

Dynamically expand the resources available for services as conditions require

Elastic Expansion — Elastic expansion enables agencies to dynamically expand the resources available for services as conditions require.

6. DNS

DNS PEP Security Capabilities

6.1. Blackholing

Protect clients from accessing malicious domains

DNS Blackholing — DNS Blackholing protections are a form of blacklisting that protect clients from accessing malicious domains by responding to DNS queries for those domains.

6.2. Domain Validation

Ensure that domain name lookups from agency clients validated

DNSSEC for Agency Clients — DNSSEC protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated.

6.3. Agency Domains

Ensure that agency domain names are secured

DNSSEC for Agency Domains — DNSSEC protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution the domain names.

7. Intrusions

Intrusion Detection PEP Security Capabilities

7.1. Endpoints

Combine endpoint and network event data to aid in the detection of malicious activity

Endpoint Detection and Response — Endpoint Detection and Response tools combine endpoint and network event data to aid in the detection of malicious activity.

7.2. Malicious Activity

Detect malicious activity, attempt to stop the activity, and report the activity

Intrusion Protection Systems (IPS) — Intrusion Protection Systems detect malicious activity, attempt to stop the activity, and report the activity.

7.3. Access

Evaluate access control decisions

Adaptive Access Control — Adaptive Access Control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.

7.4. Deceptions

Deflect attacks away from the operational systems

Deception Platforms — Deception Platform technologies provide decoy environments, from individual machines to entire networks, that can be used to deflect attacks away from the operational systems supporting agency missions/business functions.

7.5. Log Monitoring

Discover when new certificates are issued for agency domains

Certificate Transparency Log Monitoring — Certificate Transparency Log Monitoring allows agencies to discover when new certificates are issued for agency domains.

8. Enterprises

Enterprise PEP Security Capabilities

8.1. SOAR

Define, prioritize and automate the response to security incidents

Security Orchestration, Automation, and Response (SOAR) — Security Orchestration, Automation and Response tools define, prioritize and automate the response to security incidents.

8.2. Shadow IT

Detect the presence of unauthorized software and systems

Shadow IT Detection — Shadow IT Detection systems detect the presence of unauthorized software and systems in use by an agency.

8.3. VPN

Provide a secure communications mechanism between networks

VPN — Virtual Private Network solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.

Administrative Information
Start Date: 2019-12-31
End Date: 2020-01-31

Publication Date: 2020-05-20
Source: https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Vol.%203%20Security%20Capabilities%20Handbook.pdf

Submitter:
Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: