

# Incident Report

## Section 1: Type of attack that may have caused this network interruption

### **One potential explanation for the website's connection timeout error message is:**

One potential explanation for the website's connection-timeout message is a SYN-flood DoS attack that deliberately exhausts the server's backlog of half-open TCP handshakes.

### **The logs show that:**

TCP (Transmission Control Protocol) *SYN* (*Synchronize*) packets arrive in rapid succession—almost all from 203.0.113.0—with no matching final ACK (Acknowledgement)

### **This event could be:**

Classic SYN-flood DoS (Denial of Service) attack

The connection queue and worker threads are exhausted by half-open sessions

## Section 2: How the attack is causing the website to malfunction

**When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol:**

**SYN** → Client sends a SYN to open a connection.

**SYN-ACK** ← Server reserves state, replies with SYN-ACK.

**ACK** → Client completes the handshake with an ACK; the session is now fully established.

**What happens when a malicious actor sends a large number of SYN packets all at once:**

The attacker sprays millions of SYNs but never sends the final ACK, leaving the server waiting in SYN-RECEIVED state.

Each half-open session ties up a socket structure, memory, and a timer (typically 30–60 s).

Once the backlog is full, the server drops or resets new connections, so legitimate users see long page-load delays or connection-timeout errors.

**What the logs indicate and how that affects the server:**

Thousands of identical SYNs from the same host with no corresponding ACK

The server dutifully answers with SYN-ACK until its half-open queue is saturated, then begins sending RSTs and timing out valid traffic.

Legitimate IPs (e.g., 198.51.100.23) initially succeed but later receive 504

Gateway Time-out, proving resource exhaustion rather than application error.

This pattern is symptomatic of a SYN-flood DoS rather than a full Distributed DoS (DDoS (Distributed Denial of Service)), because almost all malicious traffic originates from a single (possibly spoofed) address.

### Section 3: Impact on the Organisation

**Website unavailability** – customers cannot browse or book vacation packages; employees cannot search deals.

**Revenue loss** – every minute offline during a promotion directly reduces sales.

**Reputation damage** – travelers perceive the agency as unreliable.

**Operational overhead** – emergency response, firewall reconfiguration, possible overtime, and root-cause analysis draw staff away from core work.

# Summary

The outage was caused by a **TCP SYN-flood DoS attack** that exhausted the web-server's connection backlog. Legitimate requests were queued until they timed out, resulting in the connection-timeout messages our staff and customers saw. We have temporarily blocked the offending IP, but the attacker can easily switch addresses.

**Next steps:** enable SYN-cookies or deploy a SYN-proxy at the perimeter, engage our ISP's DDoS-mitigation service, and implement rate limiting so that a single host cannot overwhelm the server again.

# Apendix A

## NIST Cybersecurity Framework (CSF) 2.0 – Overview

The **NIST CSF 2.0** is a **voluntary guidance framework** designed to help organizations of all sizes and sectors improve their **cybersecurity risk management** practices. It offers a **flexible, repeatable**, and **cost-effective** approach to managing cybersecurity risk at all levels of an organization.

### Purpose

- Help organizations identify, assess, and manage cybersecurity risks
- Promote communication between technical and non-technical stakeholders
- Support integration with broader enterprise risk management practices

### Core Components

The CSF 2.0 consists of three main components:

Component	Description
Framework Core	A set of cybersecurity outcomes and activities organized into six functions
Implementation Tiers	Describe the sophistication and maturity of an organization's cybersecurity risk management
Profiles	Help align cybersecurity activities with business objectives, risks, and needs

### Framework Core – The 6 Functions

The CSF 2.0 Core is organized into **6 high-level functions**, which represent key strategic areas of cybersecurity risk management. Each function includes **categories** and **subcategories** of outcomes.

#### 1. Govern (New in 2.0)

Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policies.

#### 2. Identify

Understand the environment to manage cybersecurity risks to systems, people, assets, and data.

#### 3. Protect

Develop and implement safeguards to ensure delivery of critical services.

#### 4. Detect

Develop and implement activities to identify the occurrence of cybersecurity events.

#### 5. Respond

Take action regarding detected cybersecurity events.

#### 6. Recover

Maintain plans for resilience and restore capabilities or services impaired due to a cybersecurity event.

### Implementation Tiers

The tiers reflect how an organization views cybersecurity risk and the processes in place to manage that risk. These tiers help organizations contextualize their practices in terms of sophistication.

Tier	Description
Tier 1	Partial – Ad hoc and sometimes reactive
Tier 2	Risk Informed – Some awareness and planning
Tier 3	Repeatable – Established policies and processes
Tier 4	Adaptive – Continuous improvement and agility

### Framework Profiles

**Profiles** are customized alignments of the Core outcomes to:

- Organizational goals
- Risk tolerance
- Regulatory requirements
- Available resources

**Current Profile:** Reflects current cybersecurity posture

**Target Profile:** Represents desired outcomes aligned with strategic goals

**Organizations use profiles to:**

- Identify gaps between current and target states
- Prioritize actions and investments
- Track progress over time

### How Organizations Use the Framework

1. Establish governance and risk management approach
2. Assess current state using the Core and Tiers

3. Develop a target profile
4. Identify and prioritize gaps
5. Implement and monitor action plans
6. Continuously evaluate and improve cybersecurity posture

**Key Benefits**

- Supports organizations of any size and sector
- Aligns with existing frameworks (ISO 27001, COBIT, etc.)
- Encourages communication across departments
- Integrates into enterprise risk management strategies
- Emphasizes continuous improvement and scalability

# Apendix B

## NIST Cybersecurity Framework (CSF) 2.0 Summary - Categories

### GOVERN

**GOVERN (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

**Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.

**Risk Management Strategy (GV.RM):** The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

**Roles, Responsibilities, and Authorities (GV.RR):** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

**Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced.

**Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

**Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

### IDENTIFY

**IDENTIFY (ID):** The organization's current cybersecurity risks are understood.

**Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.



**Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization.

**Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF Functions.

## PROTECT

**PROTECT (PR):** Safeguards to manage the organization's cybersecurity risks are used.

**Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.

**Awareness and Training (PR.AT):** The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.

**Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

**Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.

**Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.

## DETECT

**DETECT (DE):** Possible cybersecurity attacks and compromises are found and analyzed.

**Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

**Adverse Event Analysis (DE.AE):** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

## RESPOND

**RESPOND (RS):** Actions regarding a detected cybersecurity incident are taken.

**Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed.

**Incident Analysis (RS.AN):** Investigations are conducted to ensure effective response and support forensics and recovery activities.

**Incident Response Reporting and Communication (RS.CO):** Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.

**Incident Mitigation (RS.MI):** Activities are performed to prevent expansion of an event and mitigate its effects.

## RECOVER



**RECOVER (RC):** Assets and operations affected by a cybersecurity incident are restored.

**Incident Recovery Plan Execution (RC.RP):** Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.

**Incident Recovery Communication (RC.CO):** Restoration activities are coordinated with internal and external parties.

# Apendix C

## NIST Cybersecurity Framework (CSF) 2.0 – Mapping

CSF Function → Category	Scenario linkage	Strengths / Suggestions
<b>Govern (GV)</b>		
<b>GV.OC – Organizational Context</b>	The agency's business model relies on 24 × 7 public web sales; server outage directly threatens revenue.	 Business impact was immediately recognized.  Document criticality tiers or maximum tolerable downtime (MTD) for the site.
<b>GV.RM – Risk-Management Strategy</b>	DoS/DDoS is a known sector threat, yet only basic IP-block controls were in place.	Articulate Risk appetite/tolerance; Formal DoS mitigation plan.
<b>GV.RR – Roles, Responsibilities &amp; Authorities</b>	Analyst halted traffic and escalated to manager.	 Clear operational authority to take server off-line.  Incident-response roles for comms/ execs.
<b>GV.PO – Policy</b>	Temporary firewall rules were applied on the fly.	Written policy for DoS protection, SYN-cookies, or traffic-engineering controls.
<b>GV.OV – Oversight</b>	Management was notified after containment.	Board-level or audit oversight; metrics/KPIs.
<b>GV.SC – Cyber-Supply-Chain Risk Mgmt.</b>	Hosting and CDN providers could help absorb attacks.	Contracts with ISP/CDN for upstream scrubbing.
<b>Identify (ID)</b>		
<b>ID.AM – Asset Management</b>	Web server and firewall clearly inventoried.	Analyst knew which host/IP was affected.

<b>ID.RA – Risk Assessment</b>	Packet capture confirmed SYN flood versus other threats.	Rapid technical diagnosis.  Periodic threat modeling of DoS vectors.
<b>ID.IM – Improvement</b>	Opportunity to add SYN-proxy, rate-limiting.	Formal lessons-learned loop.
<b>Protect (PR)</b>		
<b>PR.AA – Identity, AuthN &amp; Access Control</b>	Not directly implicated (public site).	Upstream firewall with adaptive connection quotas.
<b>PR.AT – Awareness &amp; Training</b>	Analyst recognized flood pattern quickly.	Demonstrates effective technical training.
<b>PR.DS – Data Security</b>	Customer data remained intact; TLS (port 443) in use.	Confidentiality preserved.
<b>PR.PS – Platform Security</b>	Server accepted unlimited half-open sockets.	Need to enable SYN-cookies / tune backlog.
<b>PR.IR – Tech-Infrastructure Resilience</b>	Single web front-end became single point of failure.	Traffic scrubbing, CDN, or autoscaling for resilience.
<b>Detect (DE)</b>		
<b>DE.CM – Continuous Monitoring</b>	SIEM generated automated alert; packet sniffer used.	Monitoring caught anomaly in near-real-time.
<b>DE.AE – Adverse-Event Analysis</b>	Analyst correlated logs, packet traces, and user impact.	Good forensic skillset.
<b>Respond (RS)</b>		
<b>RS.MA – Incident Management</b>	Server taken off-line, firewall rule applied.	Timely containment.  Use of run-book.
<b>RS.AN – Incident Analysis</b>	Identified SYN flood from 203.0.113.0, classified as DoS.	Root cause determined.
<b>RS.CO – Reporting &amp; Communication</b>	Analyst plans to brief manager; internal notification only.	Address external comms (customers, ISP).
<b>RS.MI – Mitigation</b>	Blocked offending IP; recognizes spoofing risk.	Layered mitigations (rate-limit, SYN-proxy, CDN).
<b>Recover (RC)</b>		
<b>RC.RP – Incident-Recovery Plan Execution</b>	Server brought back once traffic subsided.	Quick service restoration.  Use of recovery playbook.

<b>RC.CO – Recovery Communication</b>	Manager to be briefed; customer messaging unknown.	Formal stakeholder comms; plan post-outage.
---------------------------------------	--	---