OWL Cyber Defense

USE CASE

Secure Cross Domain Data Sharing in High-Threat Environments

Summary

INDUSTRY

Intelligence / Defense

CHALLENGES

Secure data sharing between trusted networks and high threat networks (HTN)

SOLUTION

XD Bridge hardware-enforced cross domain solution

BENEFITS

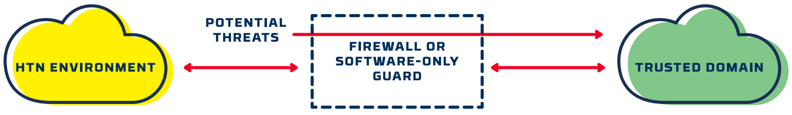
Inline filtering and hardware-enforced separation with protocol termination provide the highest possible assurance risk mitigation for data sharing with high threat networks

Cybersecurity Challenge

U.S. defense and intelligence missions and organizations are increasingly collecting and sharing information over untrusted and/or unsecured network infrastructures. These infrastructures increasingly include “high threat networks” (HTN), such as the Internet, in which a known or suspected bad actor is or could be operating without the knowledge of the primary user. HTNs are also networks that are known for a lack of sufficient cybersecurity measures or network ownership and security posture is unknown. In order to address the potential threats present in HTNs, the defense and intelligence communities require a solution that can detect and mitigate potential threats and prevent accidental or intentional disclosure of sensitive information from trusted network into the HTN.

REQUIREMENTS

- Enable secure connectivity between trusted network domains and HTNs
- Prevent data leakage and unauthorized disclosure from trusted networks, including network routing information
- Multiple, redundant content filters to detect and mitigate sophisticated, potentially novel threats from HTNs
- Hardware-enforced domain separation on each connection



Software-only network security tools susceptible to bypass / exploitation

Before Architecture

Solution

In order to meet the demands of secure cross domain transfers in high threat environments, any viable solution requires both comprehensive content filtering capabilities as well as additional safeguards to shield trusted domains from likely threat actors present in the HTN. This includes hardware-enforced domain separation, as well as a protocol termination, to prevent any network routing information from being shared between domains. The XD Bridge cross domain solution (CDS) is U.S. government-accredited, Raise-the-Bar (RTB) compliant network defense solution designed for secure data transfers between networks of differing security or trust. It provides both sophisticated software for content filtering of various data types, as well as a hardware-enforced separation and protocol break between networks.

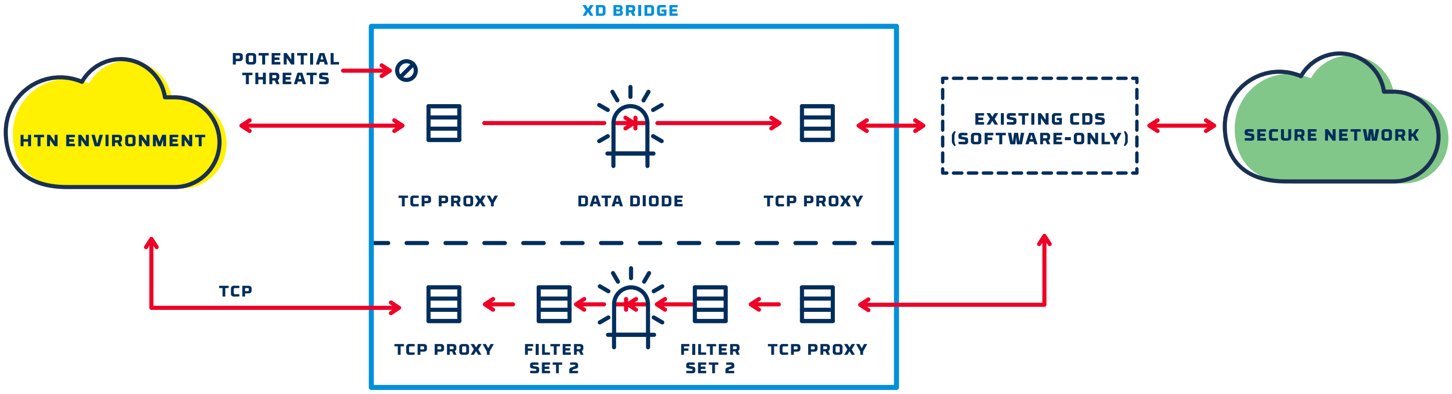
XD Bridge

XD Bridge

The premier cross domain guard platform for system integrators with application-specific needs, XD Bridge is a U.S. Government accredited, RTB compliant, ultra-high-performance cross domain solution.

Results

- Secure, high-speed data transfers between HTN and trusted domains, can be used independently to or augment existing software-based solution
- High-assurance, comprehensive, and redundant content filtering to prevent unauthorized access or sensitive data disclosure
- Built-in data diode provides a hardware-enforced network domain separation



Government accredited CDS with hardware enforced one-way data diode and filtering

OWL Cyber Defense

Owl Cyber Defense cross domain, data diode, and portable media solutions provide hardened network security checkpoints for hardened threat prevention and secure data availability. For over 20 years, Owl's unmatched expertise, products, and services have been trusted by clients in government, defense, critical infrastructure, and commercial organizations around the world.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com