TRINITYCYBER

WHITEPAPER

Zscaler’s Zero Trust Framework Reinforced and Enhanced by Trinity Cyber

Trinity Cyber redefined what's possible at the network edge, with the first ever technology that can fully open, deeply scan, treat, and rebuild full-session Internet traffic (protocol fields and files) in both directions to expose and mitigate actual threat content before it becomes an incident.

In essence, Trinity Cyber runs high-availability, real-time cybersecurity countermeasure operations as a service. It's an entirely new approach with a powerful new technology that works better and is not reliant on indicators of compromise like hashes. The new capability produces:

- Profoundly better, more accurate, and more enduring detection
- The ability to disable or remove threats before they enter or leave your network
- Less noise

Why Trinity Cyber?

- Other vendors look for, alert on, and sometimes block indicators of compromise (IOCs) – the bottom of the pyramid
- That approach is easily evaded, prone to false positives, and feeds a costly ecosystem of alert management and incident response; in other words, it's failing. According to pen testing by Positive Technologies, an external attacker can breach an organization's network perimeter in 93 percent of cases

- Trinity Cyber does not rely on indicators. Trinity Cyber invented a different solution
- Trinity Cyber tech makes it possible to sit in the middle of an internet connection and stop, decrypt, open, and examine fully assembled content in context, to accurately find and defeat hacking attempts—and no other technology can do that
- This approach works independently of IOCs and thus gives the advantage back to the defender
- Trinity Cyber's technology enables hyper-precise, highly accurate, inline operations that neutralize more threats before they become incidents—reducing risk and costs

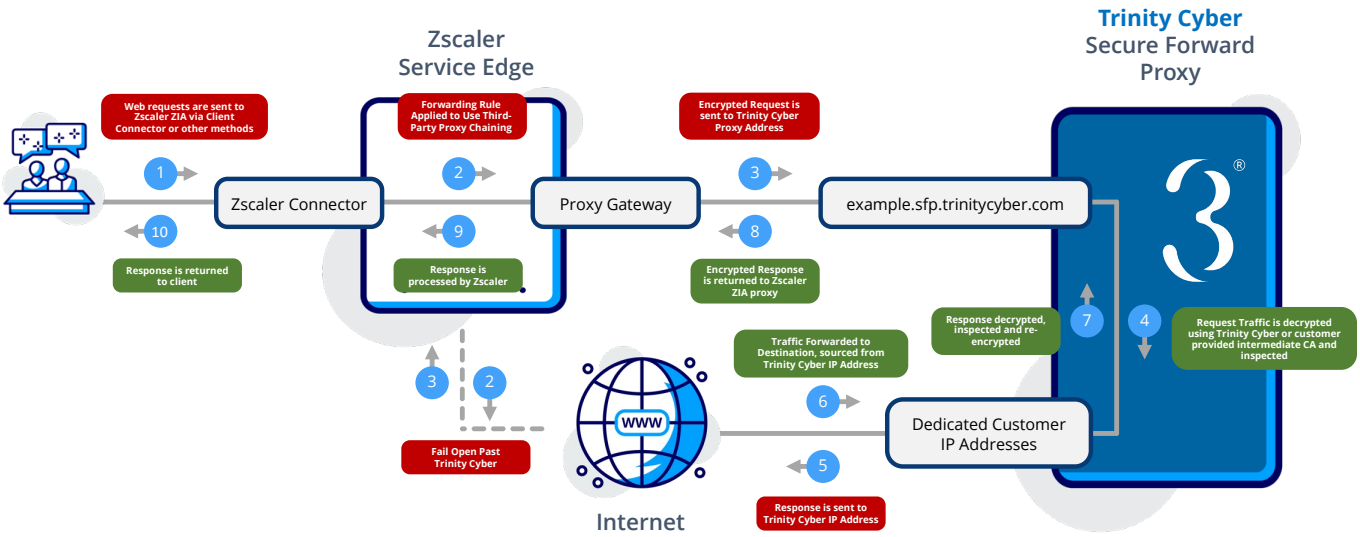
What is secure forward proxy?

The Trinity Cyber Secure Forward Proxy (SFP) connection is a straightforward way to integrate with your existing SASE solutions. It allows you to use them and Trinity Cyber, and the connection is easy. Typically, a forward proxy works as an intermediary to sit between your network and the internet. A forward proxy evaluates network requests, takes actions and then routes a request to the internet on behalf of your network. It then does the same for internet responses going back to the network. Trinity Cyber SFP does all of this, plus more. You gain the additional benefits of our full stack of cybersecurity detection and remediation as well as threat intelligence and threat hunt, a fully managed service with 24/7 support, dedicated IP space, full network session PCAP and more. The Trinity Cyber team is on hand at any time to assist with turn up, questions, and configuration.

Secure forward proxy in conjunction with Zscaler Internet Access (ZIA)

When configured using Secure Forward Proxy connectivity method, the Trinity Cyber Engine is positioned between the SASE solution and the internet, protecting the users from any inbound threats and inspecting any potentially malicious requests towards internet.

Trinity Cyber delivers a deeper, more content aware, and more enduring solution that adds significant levels of risk reduction well beyond the traditional products offered by other Zero Trust solutions (hash matching, URL filtering, and simple pattern matching). Zero Trust architectures focus on ease of use, identity management, and basic protections, but they don't provide in-depth content inspection and remediation nor prevent the delivery of new or novel malicious content without Trinity Cyber.



Zscaler's Zero Trust Framework Reinforced and Enhanced by Trinity Cyber

Along with the protections granted by Trinity Cyber, the service also provides many essential features that are not included in Zscaler deployments. Trinity Cyber will become your operational and security partner, enabling you to have an outcome driven, preventative security posture.

- **Dedicated IP Space:** Trinity Cyber Forward Proxy connector gives clients dedicated IP space which can be used on any service or website that requires IP whitelisting, while ensuring only IP space used by the client is whitelisted.
- **Full Internet Session PCAP:** Trinity Cyber provides clients with 72 hours of rolling Packet Capture on the full internet session, providing visibility into decrypted and non-decrypted sessions that leave the Zscaler environment towards the internet. This allows for both general and malware analysis on traffic and troubleshooting activities for networking teams.

- **Full Content Inspection and Remediation:** Trinity Cyber performs full content inspection and remediation inline, providing the optimal user experience – no sandboxing or delayed content delivery. Trinity Cyber understands that security posture is always a compromise between security and usability; this allows clients to disable Zscaler sandboxing if desired.
- **Fully Managed Solution as a Service:** Security posture is managed on your behalf as part of the service. The Trinity Cyber support team is available 24x7 to assist with any issues, incidents, or changes to the posture.
- **Threat Intelligence, Hunt and Discovery:** The Trinity Cyber threat and hunt teams are constantly on the lookout for zero-day threats, vulnerabilities, and Tactics, Techniques, or Procedures (TTPs) and uses multiple sources and hunting techniques:
  - The Microsoft Active Protections Program (MAPP). Trinity Cyber is a proud member of the MAPP Advance Notifications Service program, which comprises of mutual threat intelligence exchange between a very selective group of organizations, Trinity Cyber and Microsoft
  - Open Source Intelligence (OSINT) Sources
  - Other proprietary and confidential sources
  - Original discoveries that the Threat Hunt team finds in the wild
  - Threat hunting to retroactively evaluate traffic for new TTPs, zero days and obfuscation efforts

This allows us to deliver protection to you before the threats are disclosed publicly.

Straightforward Integration

Trinity Cyber service integration with Zscaler is incredibly straightforward to establish utilizing existing policies and tools in Zscaler. The Trinity Cyber support team is also available at any time to assist with integration. Turn up of the service is controlled from the client's Zscaler portal – simply configure a forwarding rule to select and steer traffic towards Trinity Cyber endpoints. Forwarding rules allow for surgical precision in selection of endpoints and traffic that a client desires to onboard.

- The onboarding pace is controlled by the client
- The forwarding rules are familiar – similar to firewall policies to select and steer traffic through Trinity Cyber
- The ability to Fail-Open or Fail-Close to fit your policy stance
- Initial turn up can be as small as a single endpoint or a group of workstations, deployment can be scaled to full production with a few clicks
- Does not conflict with Zscaler Private Access (ZPA)
- No downtime during turn up of service

The Trinity Cyber Engine integrates with Zscaler ZIA using Third-Party Proxy Chaining, which is available to all ZIA customers. The integration is completely controlled via Zscaler portal and includes 5 major steps:

1. Receive a unique endpoint address, dedicated public IP address(es) and certificate chain from Trinity Cyber. Note that endpoint address is geographically redundant – closest endpoint to the Zscaler exit node will be automatically utilized.
2. Import root certificate to Zscaler Portal and to your endpoints and Zscaler using GPO, MDM or other solutions.
3. Configure Proxies in Zscaler portal
4. Configure Proxy Gateway in Zscaler portal
5. Configure Forwarding policy and select traffic using available selectors.

For more information on the selectors, please see :
https://help.zscaler.com/zia/configuring-third-party-proxy-chaining

About Trinity Cyber

Trinity Cyber was founded in 2017 by Steve Ryan, a 32-year veteran of the NSA. In 2016, he left the agency as Deputy Director of its Threat Operations Center to start Trinity Cyber to address one major theme he noticed in his years at the NSA - indicators of compromise (IOCs) were continually changing but attacker tactics, techniques, and procedures (TTPs) were not.

Steve and the team invented and patented a groundbreaking new approach to cybersecurity that identifies, stops, and prevents threats others miss in real time. This innovative technology outperforms the components of every other network security solution and is solving the biggest challenges for customers today with better security, virtual vulnerability mitigation, reduced alert fatigue and fewer false positives.

Trinity Cyber's patented technology is the first that can deeply inspect full session internet traffic in both directions to expose and mitigate threat content inline in real time and do so while specifically targeting TTPs and not IOCs.