TRINITYCYBER

USE CASE

Branch Office

Tunnel to Trinity Cyber's Internet Gateway to Get to the Internet with the Protection of Full Content Inspection

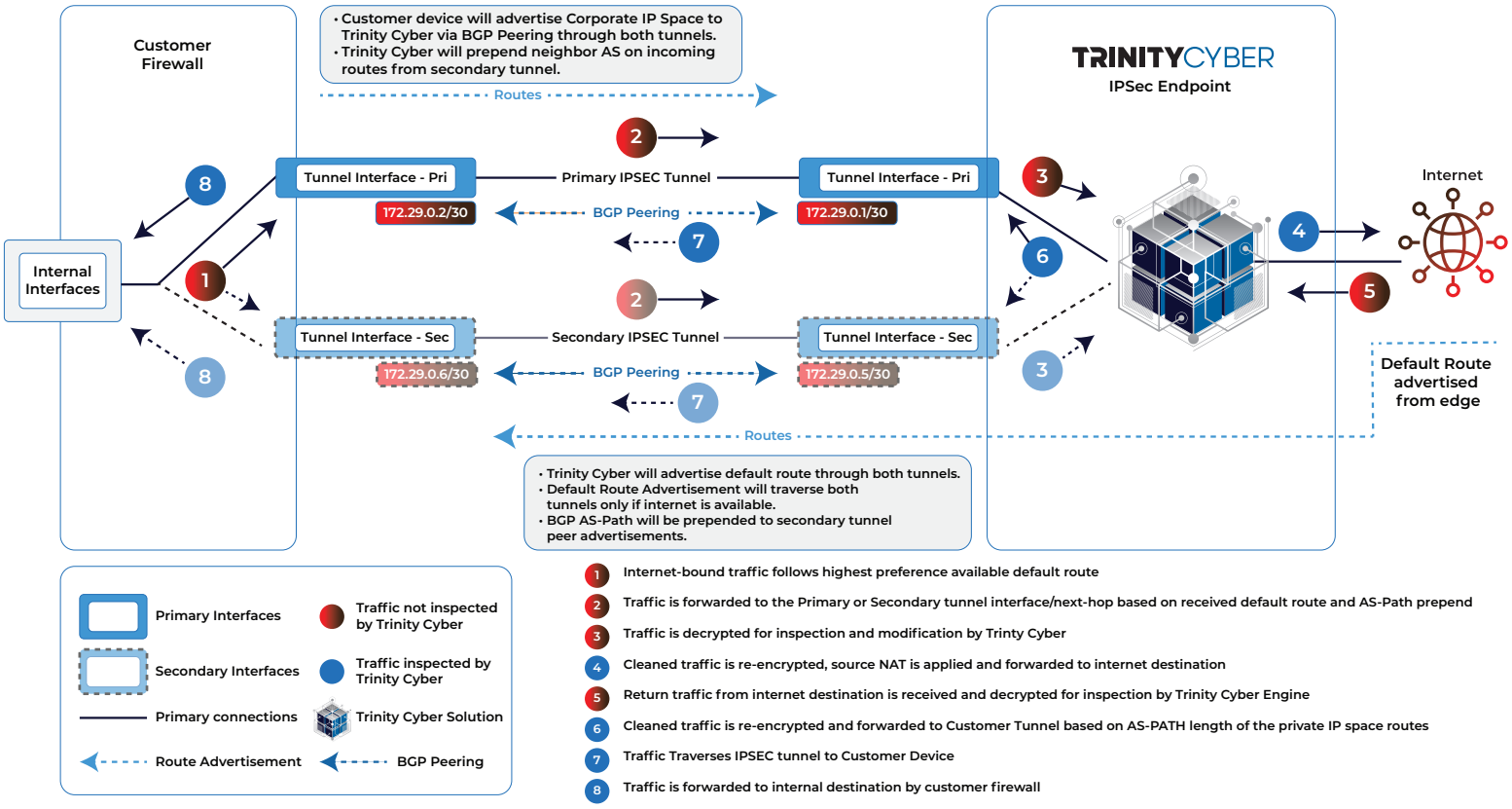
Unleash the power of Trinity Cyber's cutting-edge full content inspection technologies and team of world-class experts protecting your remote offices.

There's nothing for you to do except tunnel your branch office to one of Trinity Cyber's closest internet gateways. As soon as you are connected, your internet content is actively inspected to protect you against the ever-evolving threat landscape.

Trinity Cyber uses Internet Protocol Security (IPSec), a network protocol suite that enables secure communications between two devices over the public internet to ensure secure and authenticated tunnel connections between your branch office and the closest Trinity Cyber internet gateway. With locations in Washington, D.C.; New York; Chicago; Dallas; and San Jose, you'll get responsive and secure internet from any location in the United States. Trinity Cyber's internet gateway will be the last stop for traffic going to the internet and the first stop for incoming traffic.

There are two ways to tunnel to Trinity Cyber: A primary IPSec tunnel to a Trinity Cyber internet gateway with a backup connection that connects directly to the internet; or a primary IPSec tunnel to a Trinity Cyber internet gateway with a backup connection to the same or a different Trinity Cyber internet gateway. Consult with your Trinity Cyber customer service representative to confirm your router is on our supported devices list.

Tunnel Connectivity Using Dynamic Routing (BGP)



While an IPSec tunnel securely connects your site to Trinity Cyber, the vast majority of your web traffic is encrypted with Transport Layer Security (TLS) between your browser and the web sites you visit. It is in these encrypted channels where most cyber adversaries lurk. Trinity Cyber guides you through the easy process of installing a root certificate into the trust store of your devices to make TLS inspection possible. Trinity Cyber then decrypts your traffic; performs its full content inspection to neutralize the threats; and re-encrypts the traffic before releasing it to the internet. This entire process happens so fast, you won't even notice. Through this method, Trinity Cyber is always exposing hidden threats, while ensuring that attackers cannot exploit protected channels to infiltrate your network.

In cases where sensitive traffic cannot or should not be decrypted, Trinity Cyber manages a decryption exemption policy for you. With TLS Exemption Management, customers may identify specific segments of traffic that should remain encrypted and inaccessible. This feature is also essential for preserving the functionality of certain mobile devices. The Trinity Cyber team brings a wealth of experience to this process and offers advice on the exemptions necessary to help you run and maintain your enterprise without disruptions.

With Trinity Cyber managing your secure sockets layer (SSL) decryption, you not only receive world-class protection, but your digital forensics and incident response (DFIR) teams also get SSL-decrypted packet capture (PCAP) through the customer portal. Trinity Cyber's integrated PCAP solution enables your security team to use standard Berkeley Packet Filtering (BPF) syntax during a rolling 72-hour window, making it a breeze to search and retrieve SSL-decrypted packet captures to support thorough analysis and investigations. Your IT team will appreciate the ability to use SSL-decrypted PCAP to troubleshoot new technology integration.

As a complement to Trinity Cyber's patented technologies, the company offers standard L3 (source/destination IP) and L4 (stateful port and protocol inspection) firewall functionality, allowing you to save money by simplifying and offloading network security management. With minimal effort and Trinity Cyber at your side, you gain access to a groundbreaking, fully-managed, enterprise-level security capability without complexity and overhead – an ideal solution for anyone looking to reduce their cyber risk and increase their cybersecurity posture.

The Trinity Cyber Core Technology

Trinity Cyber's award-winning capability delivers unparalleled deep, content-based, full session inspection and real-time active cyber threat mitigation – all operated for you by an expert team of seasoned professionals. In an ecosystem overoptimized to support alert aggregation and incident response, Trinity Cyber's patented technology empowers a wide spectrum of *real-time* corrective actions – each meticulously crafted to match a CVE, threat actor group, ransomware gang, and entire families of threats. No alerts to aggregate. Near zero false positives. When the technology encounters a threat on your traffic - which it does more accurately and with a more enduring approach than any competitor in the market - it mitigates that threat on the wire, seamlessly and in real-time while delivering a context-rich notification. With average processing times of less than 1ms, neither you nor the opposition will even know the technology is there.

The technology is backed by a suite of additional cybersecurity services like content-based threat hunting and emerging threat analysis – all made better through the patented technology. Trinity Cyber operates on your behalf, defends you against the latest threats, manages all the systems, and provides you with a context-rich, interactive customer portal where you can see and drill into each and every threat stopped by the technology. Each event is fully triaged so that your security team can rest assured that not only are you protected, but that every notification in the portal is legitimate with more than 99.99% accuracy.

The portal is also home to Trinity Cyber's File Parser tool. This capability puts the power of advanced file analytics at your fingertips – security analysts can drag and drop a file and see an immediate breakout of all the file components. Customers can use it to aid in analysis, threat intelligence, and incident response. File Parser is an indispensable file submission tool designed to unearth and depict file exploits, malware, and obfuscation techniques concealed within file content.

About Trinity Cyber

Trinity Cyber runs a high-availability cybersecurity countermeasure capability as a service and triages all events as a service. You get clean traffic and less noise. It radically reduces risk and false positives. Trinity Cyber doesn't offer a secure web gateway (SWG), web application firewall (WAF), or intrusion prevention system (IPS), but rather outperforms and replaces every SWG, WAF, and IPS on the market.

Trinity Cyber sells in subscription tiers to accommodate all budgets and risk appetites. The annoying price models have died along with the old technologies that Trinity Cyber replaces. Unlimited seats for your SWG. Unlimited domains for your WAF. Internet gateway security that matches your usage. Put Trinity Cyber in your path to the internet. Pick as many connection options as you need. Only pay for what you use. Pick your tier and pay the price you see plus an additional consumption fee if applicable.

Contact us today at **Info@TrinityCyber.com** to learn more.