IronNet

WHITE PAPER

Lose Network Security Visibility or Crush Your VPN?

ADVICE FOR CISOS ON HOW TO AVOID THE NO-WIN TRADEOFF IN A 100% REMOTE-WORK MODE

By Vasanth Balakrishnan with contributions from Bill Swearingen and Zoltan Kovacs

The Current Cybersecurity Conundrum

Whether due to the current global pandemic or because of a more localized natural disaster event, companies and organizations are facing a no-win tradeoff: Do you give up full network security visibility or do you overwhelm your VPN, which may not be sized for 100% of users working remotely? Nearly all organizations are seeing a dramatic increase in the number of users working remotely to adapt to current government edicts or guidelines for remote-work and social distancing. Many of these working environments continue to use traditional Virtual Private Network (VPN) to establish secure remote connectivity back to corporate resources. Those VPN connections are coming under tremendous strain with the increased use of collaboration video tools such as Zoom or Cisco WebEx, on top of elevated traffic by users who are regularly checking news sites, YouTube, and social networks, or even using speed testing sites to check for connectivity.

In these extreme situations, network defenders — from the security analyst level up to CISO — usually have to make a difficult tradeoff:

A. Battle with your network operations team — and ultimately end-users — in order to force all user endpoint traffic into an always-on full tunnel VPN connection so that you can maintain network security visibility with your traditional datacenter on-premise network security stack (web filtering, DLP, NGFW) and increasingly next-generation platforms in the network traffic analysis (NTA) space.

OR

B. Concede that these days many mission-critical web applications, which are trusted, secure sites, do not require users to be on the VPN with the understanding that you will lose most or all of your network security visibility while the user is not connected to VPN.

Weighing Your Decisions: A Closer Look at the Options

This whitepaper will evaluate new technologies that are available and have already gained wide adoption to help resolve this network security visibility conundrum.

Acronym Guide:

VPN - Virtual Private Network
EDR - Endpoint Detection & Response
CD - Collective Defense
CISO - Chief Information Security Officer
CASB - Cloud Access Security Broker
ZTNA - Zero Trust Network access
DLP - Data Loss Prevention
SSO - Single Sign-On
SIEM - Security Information Event Manager
NGFW - Next Generation Firewall
NTA - Network Traffic Analytics
SOAR - Security Orchestration & Response

A WORD ABOUT ENDPOINT SECURITY

It is understood that a critical component to a Defense-in-Depth approach to security addressing the above tradeoff is to deploy and manage endpoint solutions such as Endpoint Detection & Response (EDR). It is acknowledged that these tools are very critical for understanding host-based processes, network connections, file/signature verification, and memory activity. Additionally the EDR systems bring a valuable tool for response. They offer the capability to sweep across all systems to identify which systems have been impacted (when something eventually does happen) and, in turn, to be able to quarantine those hosts from spreading the threat to others.

Nevertheless, there is still a lot of benefit to maintaining network traffic visibility for remote users who are leveraging your existing network security investments. Number one of these benefits is that while advanced adversaries can hide their activity and manipulate or disable endpoint security logging, the "ground truth" is in the network traffic. This activity can be detected as the adversary moves through the phases of the attack kill chain.

Cloud Security Platforms (CSPs) to the Rescue?

In the last few years, commercial cloud security platform vendors such as Zscaler, Cisco Umbrella, and Palo Alto Prisma have assertively expanded their market presence, offering a cloud-based security alternative to traditional on-premise network security (usually physical or virtual appliance-based) technologies. There is also a convergence into these areas of CASB vendors such as NetSkope taking an agent-plus-cloud approach to provide security and Single Sign On (SSO) capabilities. Nearly all emphasize a Zero Trust security framework, and some have coined the term Zero Trust Network Access (ZTNA.) This is an idea in security that narrows defenses from wide network perimeters to individuals or small groups of resources. Companies that offer ZTNA have been tremendously successful because they offer a cost and network-efficient way to scale out security capabilities to current working environments. They can be crucial in a situation where all your users have to suddenly work remotely. Most security professionals agree on the need to move toward a ZTNA framework, but it is time to start identifying problem areas:

1. By their nature, cloud-based security platforms seek to deliver good capabilities across web proxy, firewall, and DNS security domains for a broad set of customers. Necessarily, they may not address all the specific security requirements of your individual organization.
2. From an analytical suite standpoint, these platforms have to make performance tradeoffs that could limit their capabilities, such as Network Traffic Analytics (NTA), which requires computationally-intensive network traffic/log inspection and analysis.
3. **Many of the CSPs promote their "community protection" capacity. This means they can correlate threats across many customers in their platform and provide corresponding detection and mitigation capabilities. While this can be very valuable, it is not a true Collective Defense approach. Collective Defense is a platform capability that enables SOC analysts across organizations/industries/countries to collaborate on detection and response to cyber threats. Collective Defense looks across multiple defender participant networks to**

Acronym Guide:

VPN - Virtual Private Network
EDR - Endpoint Detection & Response
CD - Collective Defense
CISO - Chief Information Security Officer
CASB - Cloud Access Security Broker
ZTNA - Zero Trust Network access
DLP - Data Loss Prevention
SSO - Single Sign-On
SIEM - Security Information Event Manager
NGFW - Next Generation Firewall
NTA - Network Traffic Analytics
SOAR - Security Orchestration & Response

correlate and generate new threat intel for all participants in near real-time. Additionally, Collective Defense allows for SOC analyst live collaboration through anonymous comments.

Cloud Security and a Whitelist-Based Traffic Routing Approach

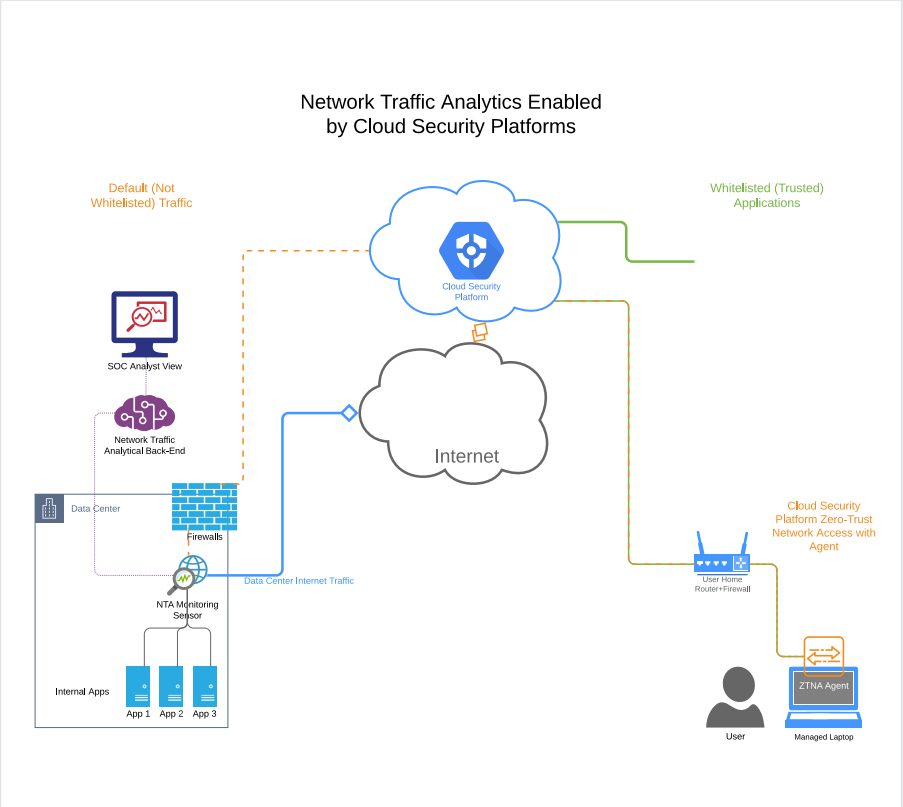
Considering how many organizations have adopted Cloud Security Platforms, there is a capability to intelligently route user traffic based on application risk using a whitelist approach. Most solutions like Zscaler offer an endpoint agent with policy management that can manage the user's endpoint network traffic to determine what traffic will be managed through their cloud platform. Traffic that is lower risk from a security perspective (e.g., YouTube, video conference / collaboration, cloud apps like Salesforce.com, Concur, etc.) could be allowed to either:

A. Be tunneled / routed to the CSP regional secure gateway for security inspection and then the closest network gateway to the cloud-based app on the internet. This is typically the default scenario.

OR

B. Route directly from the user's device out the local internet connection, which is only utilized in case of performance issues through the CSP.

All other traffic that does NOT match the whitelist can be sent over an on-demand encrypted connection for inspection by passing through the CSP regional secure gateway and then backhaul to the enterprise datacenter for in-house network security inspection. ZTNA also includes architecture configurations to allow remote users to access restricted applications available only on the corporate network, such as legacy web or thick-client applications, secure source code repositories and internal business applications.



Acronym Guide:

VPN - Virtual Private Network
EDR - Endpoint Detection & Response
CD - Collective Defense
CISO - Chief Information Security Officer
CASB - Cloud Access Security Broker
ZTNA - Zero Trust Network access
DLP - Data Loss Prevention
SSO - Single Sign-On
SIEM - Security Information Event Manager
NGFW - Next Generation Firewall
NTA - Network Traffic Analytics
SOAR - Security Orchestration & Response

ANALYSIS OF WHITELIST-BASED REMOTE USER TRAFFIC MANAGEMENT

Benefits	Drawbacks with Possible Mitigations
Delivers capability to leverage scale and network reach of your Cloud Security Provider for priority routing of lower-risk traffic	Increased management complexity of endpoint network traffic policies. *This can be greatly reduced with central management of agent policy at the CSP*
Allows network defenders to maintain security visibility and leverage sunk-cost investments for in-house network security tools	Possibly high deployment and operational cost and/or overkill. *Smaller organizations or lower cybersecurity maturity organizations may want to rely only on CSP with ZTNA*
Enables security operations teams to deploy and refine internal Network Traffic Analytics program independent of the CSP	Additional capital, OpEx, and FTE investment for NTA and assumption that CSP can support whitelist traffic management policies
Harvests the potential of collective defense independent of your CSP	Less benefit for early adopters due lack of participants vs. late comers who can benefit from greater network effects. *This framework greatly increases the traffic visibility and therefore individual participant potential value to the CD network*
Most CSPs can monitor and protect user web (HTTP, HTTPS) traffic, addressing most network threats	Email monitoring and non-web traffic may not be covered by CSP product offering.

Alternative NTA Approaches Leveraging CSPs

SEND ENDPOINT + CSP NETWORK LOGS TO NTA PLATFORM

An alternative or first-step approach to traffic whitelisting could be to send the DNS, DHCP, and web proxy logs from the CSP to your NTA platform. These could also be augmented by logs from endpoint security tools like EDR or NGAV in conjunction with a SIEM or SOAR tool.

ASSESSMENT OF LOGS-ONLY REMOTE USER NTA APPROACH

Benefits	Drawbacks
Lower end-user impact vs remote user default traffic backhaul to NTA-equipped datacenter sites	Less analytic veracity for logs compared to packets
Easier/faster implementation to send logs to NTA log-collection infrastructure	Risk that logs may be manipulated/disabled by advanced adversaries
Typically robust central logging capabilities from CSP can ease integration of logs into NTA platform	Possible inability to detect certain attack techniques and lateral movement via logs

Acronym Guide:

VPN - Virtual Private Network
EDR - Endpoint Detection & Response
CD - Collective Defense
CISO - Chief Information Security Officer
CASB - Cloud Access Security Broker
ZTNA - Zero Trust Network access
DLP - Data Loss Prevention
SSO - Single Sign-On
SIEM - Security Information Event Manager
NGFW - Next Generation Firewall
NTA - Network Traffic Analytics
SOAR - Security Orchestration & Response

USE EXISTING TRADITIONAL VPN AGENTS

Depending on the specific VPN vendor (e.g. Cisco, Palo Alto, Fortinet), there are varying capabilities of policy-based traffic management. In the past the only typical configuration was to allow traffic destined for the local subnet (typically /24 private LAN IPs) to bypass the VPN tunnel for local network printer or NAS access. Instead, some of the VPN clients may allow a more sophisticated policy based on internet domain names to route traffic over the tunnel or directly out the user's internet. In this scenario, only whitelisted traffic to specific trusted web applications would route directly to the internet with all remaining host traffic traversing the tunnel back to the regional or central datacenter with network security visibility.

ASSESSMENT OF TRADITIONAL VPN AGENT BASIC WHITELISTING APPROACH

Benefits	Drawbacks
This approach does not require investment in CSP / ZTNA	Traditional VPN agents may offer limited whitelist traffic routing functionality
Performance may be acceptable for organizations with remote users located geographically close to VPN gateways	CSP offers improved network performance and latency for trusted applications
	Complex VPN whitelisting policies will be difficult to manage and maintain

Acronym Guide:

VPN - Virtual Private Network
EDR - Endpoint Detection & Response
CD - Collective Defense
CISO - Chief Information Security Officer
CASB - Cloud Access Security Broker
ZTNA - Zero Trust Network access
DLP - Data Loss Prevention
SSO - Single Sign-On
SIEM - Security Information Event Manager
NGFW - Next Generation Firewall
NTA - Network Traffic Analytics
SOAR - Security Orchestration & Response

Summary and Implementation Planning

SUMMARY

Cloud security platforms implementing a Zero Trust Network Access model can facilitate effective Network Traffic Analytics without having a negative impact on user experience.

Effective NTA for remote users requires that high-bandwidth or latency-sensitive application traffic is not backhauled to the corporate data centers and instead routes efficiently through a CSP.

End user network log analysis enabled by centralized logging by the CSP platform is a viable alternative to NTA. Be aware of the drawbacks to behavioral analysis relying on only logs

Organizations that have not or do not plan to adopt a CSP with ZTNA capabilities may be able to use existing VPN solutions to whitelist trusted traffic, applying NTA to the remaining traffic.

IMPLEMENTATION PLANNING

Take a phased approach to roll out, addressing highest risk users first. For example, NTA visibility may be prioritized for remote users that are susceptible to phishing or have failed phishing awareness training. The Cloud Security Platform typically will feature group-based user policy management.

Discuss your behavioral network detection approach with both CSP / ZTNA technical architects and your NTA solution engineer.

For more information on our approach to Network Traffic Analytics and Collective Defense, please visit IronNet.com

About IronNet

IronNet's mission is to deliver the power of collective defense to defend companies, sectors, and nations. The company was founded in 2014 by GEN (Ret.) Keith Alexander, the former Director of the National Security Agency and founding Commander of U.S. Cyber Command. Our team consists of expert offensive and defensive cybersecurity operators with unmatched experience defending commercial and government networks against advanced threats. IronNet is backed by blue-chip investors C5 Capital, ForgePoint Capital, and Kleiner Perkins.