Cyber Tree Systems
A Business IT Solution Company

MEMORANDUM OF TRANSMITTAL

Date: September 23th, 2024
To: Chief Information Officer (CIO), Cyber Tree Systems (CTS)
From: Terrell Grenyion
Subject: Policy Review and Plan for Firewall and VPN Policy Updates

I have prepared a report titled "Policy Review and Plan for Firewall and VPN Policy Updates". This report thoroughly evaluates CTS's current firewall and VPN control policies, assesses their effectiveness, and suggests revisions to meet present and future security requirements. It starts with an analysis of the current policies in the Enterprise Information Security Policy (EISP), Issue-Specific Security Policies (ISSP), and System-Specific Security Policies (SySSP). It then recommends necessary updates to ensure that firewall and VPN systems remain strong and adaptable. Additionally, the report proposes the establishment of a new Issue-Specific Security Policy (ISSP) for Firewall and VPN Control, which will consolidate existing documents and modernize CTS’s approach to network security.

This memo serves as a cover letter for the report and emphasizes the importance of updating these policies considering technological advancements and the increasing significance of remote work.

POLICY REVIEW AND PLAN FOR FIREWALL AND VPN POLICY UPDATES

SUMMARY

As CTS continues to evolve in a digital landscape, where threats are increasingly complex and the reliance on remote work and cloud services grows, the need for strong and adaptable network security policies has never been more pressing. Firewalls and Virtual Private Networks (VPNs) serve as the cornerstone of securing the company's internal communications and data. However, the rapid changes in technology, combined with the increasing sophistication of cyber threats, require that CTS's policies be revisited to ensure they remain both comprehensive and flexible.

This report proposes a complete policy overhaul, beginning with a review of the current firewall and VPN policies across different levels of CTS's security policies. By identifying weaknesses and opportunities for improvement, we aim to create a plan that addresses both present security demands and anticipated future needs. The report recommends changes at the Enterprise Information Security Policy (EISP) level and outlines the creation of a new Issue-Specific Security Policy (ISSP) for firewall and VPN controls. This new policy will modernize CTS's security infrastructure by incorporating next-generation firewall technologies and emphasizing zero-trust security principles.

SCOPE

This report focuses on reviewing and revising the firewall and VPN control policies within the current Cyber Tree Systems (CTS) policy environment. The specific emphasis is on aligning the policies to meet modern security needs and future growth. The main areas of focus are the Enterprise Information Security Policy (EISP), Issue-Specific Security Policies (ISSP), and System-Specific Security Policies (SySSP). The goal is to ensure that CTS's network infrastructure is well-protected against evolving cyber threats and that VPN access for remote employees is secure, reliable, and scalable. This review includes the following key objectives:

First, the report identifies EISP-level provisions related to firewalls and VPNs, ensuring they align with the current security landscape, including next-generation firewall technologies and zero-trust principles. The need for stronger encryption standards and multi-factor authentication (MFA) for VPN access is also examined.

Second, a comprehensive analysis is conducted on ISSP and SySSP documents governing firewall and VPN policies, with a focus on identifying outdated or redundant provisions. This includes addressing fragmented policies and incorporating modern approaches to firewall management, such as deep packet inspection and real-time monitoring.

Third, the report provides recommendations for consolidating existing policies into a new, coherent ISSP for firewall and VPN control. Updates to related ISSPs, such as the Password Policy, Remote Access Policy, and Incident Response Policy, are also included to ensure consistency across all security policies.

Finally, a detailed plan is developed for a new Firewall and VPN Control ISSP. This plan outlines the scope, objectives, and enforcement mechanisms necessary to support CTS's current and future security needs, considering the increasing importance of VPNs in securing remote access and the adoption of next-generation firewalls.

This analysis is based on CTS's current policy framework and future security requirements, with assumptions made regarding the continued growth of remote work, the integration of cloud services, and the expanding use of advanced security technologies.

CHANGES REQUIRED IN THE EISP-LEVEL DOCUMENT

The Enterprise Information Security Policy (EISP) is CTS's main policy document, outlining the company's strategic objectives for information security. To ensure that CTS's firewall and VPN infrastructure meets both current and future demands, the following updates are recommended for the EISP:

First, the EISP must be revised to include language supporting the adoption of Next-Generation Firewall (NGFW) technologies. Traditional firewalls, which primarily focus on packet filtering and port access, are no longer sufficient to handle the growing complexity of modern threats. NGFWs provide enhanced capabilities, such as deep packet inspection, application-level control, and integrated intrusion prevention systems (IPS). These advanced features are critical in defending against sophisticated cyberattacks. Therefore, the EISP should mandate the transition to NGFWs across all of CTS's network infrastructure.

Second, the EISP must adopt a stronger emphasis on zero-trust security principles. The traditional perimeter-based approach to network security is becoming obsolete as more employees access company systems remotely and from different devices. A zero-trust architecture assumes that threats could exist both inside and outside the network and therefore requires continuous verification of all users and devices attempting to access CTS's network. By mandating zero-trust principles, the EISP will ensure that security controls are enforced at every stage of network access, regardless of the user's location or device.

Finally, the role of VPNs in remote work environments must be explicitly defined within the EISP. As CTS has shifted toward supporting a larger remote workforce, VPNs have become the primary method for securely connecting remote employees to the company's internal network. The EISP should acknowledge the increased importance of VPN technology in safeguarding remote access and specify the need for stronger security measures, such as multi-factor authentication (MFA) and real-time monitoring of VPN traffic. Additionally, the EISP should outline a requirement for continuous assessment of VPN performance and scalability to ensure that CTS can support a growing number of remote connections without compromising security.

ISSP-LEVEL DOCUMENTS TO BE RESCINDED AND REPLACED

The creation of a new Firewall and VPN Control ISSP will combine and replace several outdated or fragmented policies. The following ISSP-level documents should be rescinded and integrated into the new policy document.

The current VPN policy mainly focuses on traditional VPN protocols and access control measures. While it has been effective in the past, it does not address modern security needs, such as the rapid increase in remote work, the integration of cloud services, and the adoption of zero-trust security models. This policy will be replaced by the new ISSP, which will include updated guidelines for VPN protocols, authentication methods, and endpoint security measures. The new policy will ensure that all VPN connections are protected by the latest encryption standards and that remote devices meet minimum security requirements before being granted access.

Similarly, the existing firewall policy is limited in scope and mainly deals with basic firewall configurations, such as the use of access control lists (ACLs) and network segmentation. While these principles are still

important, they do not provide sufficient protection against today's cyber threats, which often target applications and data rather than network ports. The new ISSP will include detailed provisions for configuring NGFWs, enabling deep packet inspection, and using real-time threat detection tools to identify and block malicious traffic. By consolidating these policies into a single, coherent document, CTS will be better equipped to respond to evolving security challenges.

By rescinding these outdated policies and incorporating their relevant elements into the new ISSP, CTS will simplify its policy environment and create a unified approach to firewall and VPN security. This consolidation will also reduce administrative overhead and ensure that all employees, contractors, and third-party vendors follow consistent security protocols.

CHANGES NEEDED FOR REMAINING ISSP-LEVEL DOCUMENTS

Some policies will be revoked, while others will need specific updates to comply with the new Firewall and VPN Control ISSP. The recommended changes for the remaining ISSP-level documents are as follows:

First, the Password Policy should be updated to require multi-factor authentication (MFA) as a standard security measure for VPN access. MFA adds an extra layer of security by mandating users to provide two or more forms of authentication, such as a password and a verification code sent to their mobile device. Given the heightened risk associated with remote access, especially when using unsecured networks, MFA should be mandatory for all users accessing the CTS network via VPN. Additionally, the policy should enforce stricter password complexity requirements for VPN users to prevent brute-force attacks.

Second, the Remote Access Policy needs to include the zero-trust principles outlined in the new ISSP. This involves continuous monitoring and verification of remote users, as well as ensuring that all devices connecting to the CTS network through a VPN meet minimum security standards, such as up-to-date antivirus software and endpoint detection and response (EDR) solutions. Furthermore, the remote access policy should prohibit the use of split-tunneling, which can expose CTS's network to risks by allowing traffic to bypass the VPN tunnel.

Finally, the Incident Response Policy must be revised to include procedures for handling firewall and VPN-related incidents. The policy should mandate real-time monitoring of firewall logs and VPN connections, allowing the Incident Response Team (IRT) to detect and respond to security breaches as soon as they occur. This will improve CTS's ability to mitigate damage caused by firewall misconfigurations, VPN vulnerabilities, or unauthorized access attempts. By updating the incident response policy to account for these specific risks, CTS can reduce the likelihood of prolonged downtime or data loss resulting from network breaches.

PLAN FOR THE NEW ISSP: FIREWALL AND VPN CONTROL POLICY

The new Firewall and VPN Control ISSP will serve as the guiding document for configuring, managing, and securing CTS's firewall and VPN infrastructure. The policy aims to ensure that all network traffic passing through CTS's firewalls and VPNs is adequately protected from unauthorized access, data breaches, and cyberattacks, supporting the company's strategic goals by securing both internal and external network communications. The policy applies to all CTS employees, contractors, third-party vendors, and external partners who access the company's network through firewall-protected systems or VPN connections. It encompasses the use of both traditional and next-generation firewall technologies, as well as modern VPN protocols and encryption standards. By adhering to this policy, CTS will maintain a secure, scalable, and resilient network infrastructure that can adapt to evolving security threats and support the company's growing remote workforce.

Annotated Outline for the ISSP:

1. **Purpose**
   This section will define the objectives of the Firewall and VPN Control Policy, explaining its role in safeguarding CTS's network infrastructure. It will highlight the importance of protecting internal communications and preventing unauthorized access to sensitive data.
2. **Scope**
   This section will specify the individuals, systems, and devices subject to the policy. It will outline the responsibilities of employees, contractors, and third-party vendors in adhering to firewall and VPN security standards.
3. **Firewall Policy**
   This section will describe the different types of firewalls in use, including traditional firewalls and next-generation firewalls (NGFWs). It will provide guidelines for configuring firewalls to enable secure network segmentation, deep packet inspection, and real-time threat detection. Additionally, it will outline best practices for monitoring firewall logs and ensuring that all traffic is inspected for potential threats.
4. **VPN Policy**
   This section will outline the requirements for secure VPN connections, including the use of approved VPN protocols (IPSec, OpenVPN, L2TP) and encryption standards. It will also mandate the use of multi-factor authentication (MFA) for all VPN users and prohibit the use of split-tunneling to prevent unauthorized traffic from bypassing the secure VPN tunnel.
5. **Zero-Trust Principles**
   This section will emphasize the importance of zero-trust security models, which require continuous verification of users and devices before granting network access. It will outline policies for enforcing endpoint security, ensuring that all remote devices meet minimum security standards, and monitoring network traffic for suspicious activity.
6. **Enforcement and Compliance**
   This section will outline the consequences of non-compliance with the Firewall and VPN Control Policy, including disciplinary action for employees who fail to adhere to the policy. It will also specify the auditing and monitoring processes that will be used to ensure compliance.
7. **Review and Updates**
   This section will describe the process for reviewing and updating the policy to ensure that it remains relevant and effective in the face of evolving security threats. The policy will be reviewed annually, with updates made as necessary to reflect changes in technology and industry best practices.

CONCLUSION

The recommendations in this report aim to enhance CTS's firewall and VPN policies to ensure that the company's network infrastructure remains secure, scalable, and adaptable to future challenges. By consolidating outdated policies into a single, comprehensive ISSP, CTS will improve its ability to manage firewalls and VPNs consistently and efficiently. Furthermore, the proposed updates to the EISP and other ISSP-level documents will ensure that all security policies align with modern technologies and best practices. These efforts will better position CTS to protect its network from cyber threats and support its growing remote workforce.