UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET, INC.,

Petitioner,

v.

NETSKOPE, INC.,

Patent Owner.

U.S. Patent No. 8,397,282

Case No.: IPR2026-00041

NETSKOPE, INC.'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

EXHIBIT LIST

No.	Exhibit Description
Ex. 2001	Scheduling Order for Netskope, Inc. v. Fortinet, Inc., Case No. 4:25-cv-02360-HSG, pending in the United States District Court for the Northern District of California.
Ex. 2002	Fortinet Inc.'s Preliminary Invalidity Contentions in Netskope, Inc. v. Fortinet, Inc., Case No. 4:25-cv-02360-HSG, pending in the United States District Court for the Northern District of California.
Ex. 2003	Exhibit A-1 of Fortinet Inc.'s Preliminary Invalidity Contentions in Netskope, Inc. v. Fortinet, Inc., Case No. 4:25-cv-02360-HSG, pending in the United States District Court for the Northern District of California.
Ex. 2004	Plot from Docket Navigator – Profile of Judge Haywood S. Gilliam Motion Success To Stay Pending IPR
Ex. 2005	Plots from Docket Navigator – Profile of Judge Haywood S. Gilliam Time to Milestones (annotated)
Ex. 2006	Website blog on Fortinet.com, titled: "Fortinet is Leading Innovation in the Security Industry with More Than 1,500 Patents" https://www.fortinet.com/blog/business-and-technology/fortinet-is-the-security-innovation-leader-more-than-1500-patents-either-awarded-or-pending
Ex. 2007	Website article on Wikipedia.org, titled: "Fortinet" https://en.wikipedia.org/wiki/Fortinet
Ex. 2008	U.S. Patent No. 9,894,100
Ex. 2009	File History of U.S. Patent Application No. 14/566,403
NEW EXHIBITS	
Ex. 2010	Declaration of Dr. Michael Franz, Sc.D.

I. INTRODUCTION

Patent Owner Netskope, Inc. ("Patent Owner") respectfully submits this Preliminary Response to the Petition for *Inter Partes Review* ("IPR") filed by Fortinet, Inc. ("Petitioner") challenging claims 1-35 ("Challenged Claims") of U.S. Patent No. 8,397,282 ("the '282 patent") based on three grounds.

The '282 patent describes a dynamically self-configurable firewall using a conceptual model in which network traffic is represented as flows between "nodes" along with a dynamically adaptable set of rules organized in a hierarchical structure that specify how the traffic should behave. The specification explains that the novel model lets an owner generally describe the firewall's behavior and the system automatically generates the specific configuration. '282 patent, 2:50-55, 7:1-4. The firewall's chains of rules form various paths through this hierarchical structure and provide defined places for adapting the set of firewall rules during runtime without operator interaction. *Id*., 2:46-55, 3:5-9, 5:5-9. Adaptations include automatic insertion, deletion, and modification of rules at these defined update points. *Id*., Abstract, Claims 1, 12 and 24.

The hierarchical structure of the dynamically adaptable set of rules includes ":A" (arriving), ":M" (matrix), ":D" (departing), and ":X" (extension) subtrees, where the "X" chains serve as well-defined taps into the main firewall chains for dynamic updates while the firewall is running. *Id*., 5:5-9, 7:5-12, 7:44-8:4. The

specification explains that an owner "generally describe how the firewall should behave," and the system automatically generates the specific configuration, eliminating detailed manipulation by a human operator. *Id*., 2:50-55, 7:1-4. Network interface devices can be associated with a node and assigned same behaviors as other devices in that node, such that data flowing "between devices can be monitored and controlled according to the behaviors and rules of each device." *Id*., 2:56-64.

Accordingly, the claims of the '282 patent properly capture the adaptive network firewall architecture and solution provided by the '282 patent. Independent Claim 1, for instance, requires, *inter alia*, "*the set of firewall rules is dynamically self-configurable during runtime without operator interaction*," "*the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure*," and "*wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime*." Claims 12 and 24, the other independent claims of the '282 patent, recite similar features as Claim 1 and are respectively corresponding device and computer-readable medium claims.

Overall, the merits of the Petition are deficient, and its arguments are confusing and inconsistent for most, if not all, claim elements. The Petition fails to demonstrate a reasonable likelihood that Petitioner would prevail in showing that

any of the Challenged Claims is unpatentable. Rather than presenting a coherent, evidence-based obviousness or anticipation case, the Petition relies on strained reinterpretations of the prior art, conclusory expert assertions, and a piecemeal reconstruction of the '282 patent using hindsight. As explained below, Coss does not anticipate or render obvious the core claim requirements of the '282 patent. Accordingly, the Board should deny the Petition under 35 U.S.C. § 314.

II. LEVEL OF ORDINARY SKILL IN THE ART

The Petition and its Petitioner's Expert Declaration, describes a person of ordinary skill in the art (POSITA) as "an individual with either (1) at least a bachelor's degree in computer science or computer engineering or an equivalent field plus at least one year of experience working on computer networking, or (2) at least 3 years of experience working on computer networking, even without a formal degree." Petition at 7, Ex. 1003, ¶¶16-20.

For the purposes of this Preliminary Response, Patent Owner relies on the definition proposed by Petitioner because Petitioner has not shown that any challenged claim is unpatentable even under this level of skill.

III. CLAIM CONSTRUCTION

For the purposes of this Preliminary Response, Patent Owner believes all claim terms should be interpreted in their plain and ordinary meaning.

In particular, Petitioner's proposed construction for "*wherein the set of*

firewall rules is dynamically self-configurable during runtime" improperly narrows the scope of the claim because if fundamentally misinterprets the claim limitation. The relevant portion of claim 1 states (similarly recited in Claims 12 and 24):

> *and accepting or denying the packet based on the set of firewall rules,* ***wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction****, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.*

The Petitioner's proposed construction makes two improper changes that the Board should reject: (1) that "*self-configurable*" requires absolutely no human operator interaction, and (2) that the firewall rules be configured while the node is evaluating whether to accept or deny the packet. *See* Petition at 7-8. Neither assertion has support in the claim language, the specification, or the prosecution history.

First, the specification provides direct support for the firewall being self-configurable while still allowing some operator interaction. "Embodiments disclosed herein relate generally to network firewall designs and methodologies and more specifically to network firewalls that can dynamically adapt to changing conditions and operator requirements." '282 Patent, 1:35-28. This passage confirms

that operators may modify rules that influence the firewall configuration, contradicting the Petitioner's assertion of zero operator involvement. Petitioner's construction improperly conflates the firewall's ability to be configured without operator interaction with a requirement where no human operator interaction can occur at any point. Such a construction not only contradicts the specification's explicit teachings but also improperly limits the claim such that any human modification—even an initial configuration—would render the firewall non-dynamic.

Second, the dynamic firewall's self-configuration need only be during runtime—not while a node is actively evaluating whether to accept or deny a packet. This limitation reflects that the accepting or denying relies on the set of firewall rules rather than assigning when the configuration must occur. This is supported by the "*wherein*" that follows the limitation describing how the firewall rules are modified rather than stipulating whether the packets are accepted or denied.

The specification reinforces this understanding. "One main embodiment of the invention is the ability to dynamically extend, prune or otherwise modify these firewall rule chain sets as functional requirements or the network operation environment changes." '282 Patent, 6:60-7:4. Dynamic configuration does not need to occur only when a packet is waiting to be accepted or denied; it can occur at any point during runtime when conditions change.

The Petitioner's construction also conflicts with the dependent claims. For example, dependent claim 7 confirms no other steps occur between receiving the packet and accepting or denying the packet: "*A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules*." '282 Patent, Claim 7. This language confirms that, within the independent claims, the firewall rules do not need to be configured while a packet is being evaluated—if the packet is being conditioned based on the firewall's rules, those rules must already exist. The Petition cites generally to the Applicant's remarks and amendments during prosecution as allegedly supporting its construction. Petition at 7-8. However, the remarks repeatedly state that the distinction between the claim language and the prior art is that the claims reconfigure the firewall at runtime—nothing more. *See* Ex. 1002, 617-19. Nothing in the record, implicitly or explicitly, supports Fortinet's proposed construction.

Because the claim language, specification, and prosecution history all confirm that Fortinet's construction is incorrect, the Board should adopt the plain and ordinary meaning of "*wherein the set of firewall rules is dynamically self-configurable during runtime*."

However, the Petitioner has not shown that any challenged claim is unpatentable even under either the terms' plain and ordinary meaning or the

definitions proposed by the Petitioner.

IV. THE CHALLENGED CLAIMS ARE PATENTABLE OVER THE TEACHINGS OF COSS ALONE OR IN COMBINATION WITH KE

A. Coss fails to anticipate or render obvious multiple claimed elements and limitations of independent Claims 1, 12, and 24 in Grounds 1 and 2

Petitioner contends that independent claims 1, 12, and 24 are anticipated and/or rendered obvious by Coss alone under pre-AIA 35 U.S.C. § 102 or § 103. *See* Petition at 3. These assertions are incorrect. As demonstrated below, Coss fails to teach or suggest several claimed features, and therefore cannot anticipate or render obvious any of the challenged claims.

A claim is only unpatentable under 35 U.S.C. § 102 if "each and every element as set forth in the claim is found . . . in a single prior art reference." MPEP 2131; *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, (Fed. Cir. 1987). For obviousness, the Supreme Court in *KSR International Co. v. Teleflex Inc*. reaffirmed that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." MPEP 2141; *KSR*., 550 U.S. 398, 416 (2007). Grounds 1 and 2 fail as a matter of law to satisfy these standards, and they do not even attempt to identify each claim element and its corresponding limitations, relying instead on conclusory, ipse dixit mappings.

Grounds 1 and 2, which rely on Coss alone, either ignore numerous elements or offer opaque and incorrect mappings. For brevity, we highlight only a few of the most glaring deficiencies below. Ex. 2010, ¶51.

1. Coss does not disclose, teach, suggest, or render obvious the claimed "*defining at least one node, wherein the at least one node is associated with two or more network interfaces*" in 1[a], 12[c][i], and 24[a] of Claims 1, 12, and 24, respectively.

Coss does not disclose, teach, suggest, or render obvious at least the claimed "*defining at least one node, wherein the at least one node is associated with two or more network interfaces*" in limitation 1[a] of Claim 1, and similarly in parallel limitations 12[c][i] and 24[a] of Claims 12 and 24, respectively. Ex. 2010, ¶52.

Petitioner maps Coss's "domains," "sub-sites," LANs, and subnets as the claimed "node," contending that Coss's discussion of multiple security domains and a domain table in Figure 6 proves that the claimed "*defining*" is satisfied. Petition at 14-16. The Petition further points to the domain entries and leans on expert's say-so, without providing any objective evidence. *See* Petition at 15-16, 23-24 citing Ex-1003, ¶¶67-68. In short, Petitioner maps Coss's domain to the claimed "*node*," and then infers the missing "*defining*" step from generic descriptions of preexisting domains and rule processing. Petition at 15-16.

Petitioner's mapping fails at least because Coss does not teach or suggest "*at least one node*." Petitioner attempts to fill that hole with generalized domain

concepts and a domain table from Coss (i.e., Fig. 6, reproduced below) that, at most, shows administrative convenience for listing or grouping resources. Petition at 16 citing Ex. 1004, 7:10-15 ("***For convenient linking of each network interface to a domain***, a domain table is used") (emphasis added). That is attorney argument and not an express or necessarily present disclosure of the claimed "*defining*" step. Anticipation requires the latter, and Petitioner failed to meet that standard.

In Coss, the term "domain" refers to a defined subpart of a network topology. For example, Coss's Figures 1 and 6 (annotated and reproduced below) illustrate that the overall network is partitioned into domains, each assigned a separate region of the IP address space. Ex. 1004, 3:43-57, 7:10-14, Figs. 1 and 6; Ex. 2010, ¶53.

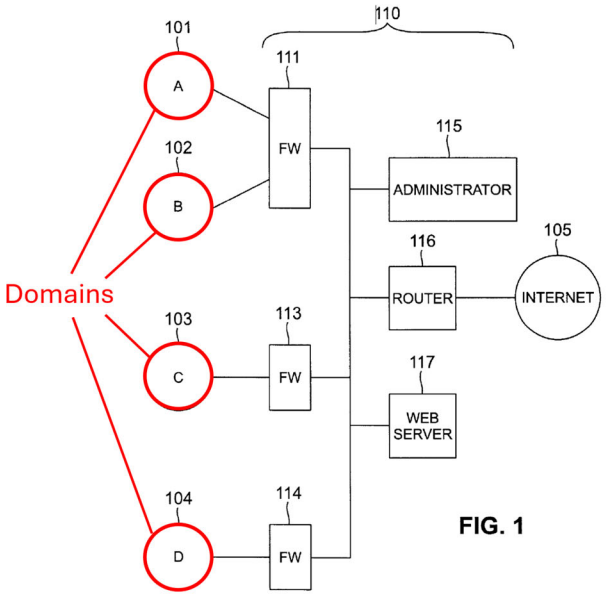

FIG. 1

INTERFACE	ADDRESS RANGE	DOMAIN
0	10.50.0.0 - 10.50.255.255	A
0	10.60.0.0 - 10.60.255.255	B
1	*	C
2	*	*

FIG. 6

Annotated Fig. 1 of Coss

Annotated Fig. 6 of Coss

Conversely, in the '282 Patent, a "*node*" is a logical concept used to model behaviors. For example, a "*node*" can contain any number of services and devices, and devices are expressly moved between nodes to change their behavior. *See e.g.*, '282 patent, 5:30-35. A "service" is a set of rules that operate on packets in specific ways, such as masquerading outgoing packets or capturing incoming packets. *Id*., 9:3-5. When a device is moved from one node to another, the move deletes the device's existing behaviors and states and assigns new ones. *Id*., 5:39-43. The '282 Patent further teaches that new devices are introduced to the firewall by first placing them in the "Null node," which has no services (behaviors), and then explicitly moving them to another node. *Id*., 5:36-43; Ex. 2010, ¶54.

In contrast, Coss does not teach "moving" devices because it does not use nodes. Its concept of a "domain" (which Petitioner maps onto a "node") reflects an aspect of network topology, not behavior. Specifically, Coss refers to "user sites or domains" in Fig. 1 and to "security domains" (*see* Petition at 14-15 citing Ex. 1004, 3:36-4:3), but a POSITA would have understood that Coss's domains or security domains are fundamentally different from the "nodes" described in the '282 Patent, which can be logical behavior constructs among which devices are moved to change their behavior. Ex. 2010, ¶55. As explained by Dr. Franz, the '282 patent introduces nodes as a way of associating devices with behaviors which can occur when a device is "moved" to the node. *Id*. Nodes and their associated behaviors form part of an

automated system that enables a firewall owner to "generally describe how the firewall should behave, and the automated system can automatically produce the requisite, specific firewall configuration, without detailed manipulation by a human operator." '282 patent, 2:50-55; Ex. 2010, ¶56.

Further, the Petition repeatedly contends that Coss "discloses, and at minimum renders obvious" element 1[a], but the Petition never identifies where Coss suggested performing a step of defining a node in the claimed method, and instead relies on POSITA inferences to transform background descriptions of domains into the claimed act of "*defining*" a node. Petition at 14-15. The Petition further leans on expert say-so without providing any objective evidence that a POSITA would have understood the claimed defining step from the existence of domain entries, simply because "a system typically cannot protect an undefined entity." *Id*. at 15 citing Ex-1003, ¶¶67-68. Petitioner's resort to Ke in Ground 3 to patch the hole only underscores that Coss alone does not disclose or suggest this limitation.

Accordingly, Coss fails to teach or suggest "*defining at least one node, wherein the at least one node is associated with two or more network interfaces*" in limitations 1[a], 12[c][i], and 24[a] of Claims 1, 12, and 24, respectively. Ex. 2010, ¶57.

2. Coss does not disclose, teach, suggest, or render obvious the claimed "*wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction*" in limitations 1[d], 12[b], and 24[d] of Claims 1, 12, and 24, respectively.

Petitioner maps the "*dynamically self-configurable during runtime without operator interaction*" clause to Coss's "dynamic rules," pointing to language that such rules "can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator," and to the proxy-reflection flow in which, at step 1012, "the firewall loads a dynamic rule," as supposed proof of self-configuration without operator interaction. Petition at 24-26 (citing Ex. 1004, 8:27-59; 9:28-10:21; Claim 35). Petitioner then relies on the expert declaration for its obviousness argument to contend that, because Coss distinguishes a "trusted application" from a "firewall administrator," dynamic rules are loaded "without human intervention," and thus teaches or suggests the claimed "*self-configurable during runtime without operator interaction*." Petition at 24-26 citing Ex. 1003, ¶¶76-77.

Coss does not disclose or suggest the claim limitation and the Petitioner's anticipation case fails at the threshold. As explained below, Petitioner's mapping never identifies any Coss disclosure where the rule set configures itself, let alone does so without operator interaction. Ex. 2010, ¶58.

Coss's "dynamic rules" already contain "unique, current information such as, for example, ***specific source and destination port numbers***." Ex. 1004, 8:27-59 (emphasis added). These "dynamic rules" are provided and loaded by "trusted application" or "trusted parties"—including a "firewall administrator" and a "remote proxy" and not by the rule set configuring itself—which is different from "*self-configurable*" and "*without operator interaction*." *See e.g.*, Ex. 1004, 8:27-59; Ex. 2010, ¶59. Nothing in that disclosure states that Coss's firewall is "*self-configurable*," and to the contrary, "trusted applications" or "trusted parties" supply the configuration change. *See id*. Anticipation requires the limitation to be expressly or necessarily disclosed, and Coss's reliance on trusted parties—including a firewall administrator—contradicts the claimed limitation of "*without operator interaction*."

Petitioner's step-1012 citation (Petition at 25) does not rescue its theory. Coss's step 1012 merely states—in its entirety—that "the firewall loads a dynamic rule to perform this action." Ex. 1004, 10:7-8. Nowhere does step 1012 disclose or suggest that the firewall is configurable, let alone "*self-configurable*," during this step. Anticipation and obviousness arguments fail because Petitioner never pinpoints a Coss disclosure where the firewall rules are "*self-configurable*" and "*without operator interaction*," nor any disclosure in Coss that suggests such feature.

Petitioner's reliance on the words "trusted application" (Petition at 24-25) to imply no operator interaction ignores the separate "*self-configurable*" requirement,

yet it still fails to identify any "*self-configurable*" mechanism or any self-configuration during running time. Even if Petitioner pivots to obviousness, the POSITA gloss still collapses. Devoid of any objective evidence, the expert's ipse dixit that distinguishing a "trusted application" from a "firewall administrator" somehow establishes "*without operator interaction*" is speculation. *See e.g.*, Ex-1003, ¶77. The Petition proffered no articulated motivation or reasoned pathway in Coss to convert loading Coss's "dynamic rules" into "*set of firewall rules [that] is dynamically self-configurable*," and no explanation of how the Coss architecture—which depends on trusted parties to load rules—would inherently or obviously operate without operator interaction.

Indeed, as Patent Owner's expert Dr. Franz explains, the '282 patent's automatic self-configuration based on a general description of "how the firewall should behave" ('282 patent, 2:50-52") is clearly different from Coss's usage of a trusted application acting as an agent of a human "operator" or being an "operator" all in itself. Ex. 2010, ¶60. Specifically, the '282 patent uses the language of "*self-configurable*," not just in the claim language, but also in other places in the patent, such as: "Dynamic firewalls can monitor transient network client connections and adjust ***themselves*** to optimally serve and protect a dynamically changing network client population on both 'sides' of a firewall." '282 patent, 2:35-38 (emphasis added). "[T]he automated system can ***automatically*** produce the requisite, specific

firewall configuration", based on a general description of how the firewall should behave. *Id*., 2:50-55 (emphasis added). As Dr. Franz opined, one of the innovations described in the '282 patent is that this behavior can be modeled using "nodes" — as devices move between nodes, their behavior changes, and then, "the automated system can automatically produce the requisite, specific firewall configuration." Ex. 2010, ¶59-61.

Therefore, Petitioner's anticipation or obviousness assertions for "*dynamically self-configurable during runtime without operator interaction*" of 1[d], 12[b], and 24[d] of Claims 1, 12, and 24 respectively, are deficient and lack underlying support in Coss. This failure confirms that Petitioner has not met its burden to show a reasonable likelihood of prevailing on this ground based on either anticipation or obviousness theories, and institution should be denied.

3. Coss does not disclose, teach, suggest, or render obvious the claimed "*wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure*" and "*wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime*" in limitations 1[d], 12[b], and 24[b] of Claims 1, 12, and 24 respectively.

Coss does not disclose, teach, suggest, or render obvious at least the claimed "*wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure*" and "*wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules*

during runtime" in limitations 1[d] of Claim 1, and similarly in parallel limitations 12[b] and 24[b] of Claims 12 and 24, respectively. Ex. 2010, ¶62.

Petitioner maps the "*plurality of chains of rules forming various paths through a hierarchical structure*" to Coss's sequential rule tables and two-domain lookups, asserting that Figures 3 and 5A-5B show different "paths" depending on whether source- or destination-domain rules match, and therefore disclose a hierarchical structure of chains and paths. Petition at 21-24. According to Petitioner, applying one of several "distinct sets of access rules" and moving from the source-domain rules to the destination-domain rules establishes a hierarchical structure, and Figure 3's tabular rules "applied sequentially" supposedly teach or suggest "chains" that together form paths through that hierarchical structure. Petition at 20-24 (citing Ex. 1004, 1:61-2:6; 4:4-19; 4:27-37; 6:18-65; Figs. 3, 5A-5B). Petitioner's mapping overreaches and ignores what Coss actually discloses: a flat, linear rule table processed sequentially, ***not*** a hierarchical structure as claimed.

Coss's rule processing is expressly tabular, not hierarchical. Specifically, Coss represents security policies as "sets of access rules" in "tabular form," and "the rules are applied sequentially until a rule is found which is satisfied…(or until the rule table is exhausted)," which is a representation of a flat list rather than a tree or hierarchical structure. *See* Ex. 1004, 4:4-19; 4:27-37. Similarly, Figure 3 of Coss (annotated and reproduced below) merely depicts a single table of rules and

categories, rather than describing a hierarchical structure. Ex. 1004, 4:4-37, Fig. 3. The Petition's reliance on Figure 3's tabular rule table and the statement that the "particular rule set…can be determined" based on interfaces and addresses (Petition at 20-24 (citing Ex. 1003, ¶76; Ex. 1004, 1:61-2:6)), at most shows selection among flat rule sets, not "*various paths through a hierarchical structure*" as claimed.

RULE NO.	SOURCE HOST	DEST. HOST	SERVICE	ACTION
10	A	B	FTP	PASS
20	A	*	*	DROP
30	B	C	TELNET	PROXY
40	*	D	MAIL	PASS

FIG. 3

Annotated Fig. 3 of Coss

Petitioner's reliance on Figure 5A-5B fares no better: that flowchart shows a series of discrete lookups and domain-matching processes, not "*various paths through a hierarchical structure*" as claimed. *See e.g.*, Ex. 1004, 1 6:18-7:9; Figs. 5A-5B. Determining which domain the packet is supposed to cross and examining applicable rules do not convert a flat rule table into a "*a plurality of chains of rules forming various paths through a hierarchical structure*" as the claims require. *See e.g.*, Ex. 1004, ("Such processing includes determining the domains which the

packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required.").

In contrast, the '282 patent provides detailed examples of hierarchical structures. For example, Fig 2. of the '282 patent (divided into Figs. 2A and 2B) describes tree/subtree structure that includes chains with the concept of "calling" and "return" targets. *See e.g.*, '282 patent, 5:5-14, 6:36-9:2, 8:5-65, Fig. 2.

As Dr. Franz explains, Figs. 2A and 2B shows leaf chains whose suffixes indicate their behavior, such as ":Accept" chains at 210 with ACCEPT targets and when a packet matches one it "**immediately jumps out of the subtree** , and moves to the next" ('282 patent, 8:5-21, emphasis added); ":Pass" chains at 214 have RETURN targets and a single DROP at the end with a RETURN target causing the packet to jump out of the current chain and "resume its path through the '**calling'** chain" (*id*., 8:29-33, emphasis added); ":Skip" chains contain rules with RETURN targets and "[p]ackets that match none of the RETURN rules are processed by the final rule" (*id*., 8:57-65). These chains form a tree with depth and structured decision logic with controlled exits that form a hierarchical structure. Ex. 2010, ¶¶63-64. As Dr. Franz confirmed, the chains of the '282 patent are not merely "flat" serialized sequences connected via jumps from one chain to another, but also includes the hierarchical rule processing flow with "calling" and "returning" semantics (a pushdown automaton) that form various paths through a hierarchical structure. *Id*.,

¶65-66. Further, within this hierarchical structure, tap locations are provided for dynamically updating the set of firewall rules during runtime. *Id*. Ex. 2010, ¶65-67.

Accordingly, Claims 1, 12, and 24 cannot be anticipated by or rendered obvious by Coss when there are numerous claim elements and limitations absent in the cited reference. The fact that the Petition fails to identify multiple claim features in the reference is indicative of the reference's individual and collective lack of teaching. Claims 1, 12, and 24 are patentable over Coss, and therefore their dependent claims are too. Thus, *inter partes* review of the '282 patent is unwarranted.

4. Dependent Claims 2-11, 13-23, and 25-35 are not anticipated or rendered obvious by Coss for at least the same reasons as independent Claims 1, 12, and 24, respectively.

For at least the reasons articulated above for independent claims 1, 12, and 24, dependent claims 2-11, 13-23, and 25-35 are also novel over Coss.

B. There is no motivation to combine Coss and Ke

Ke is generally directed at performing firewall and routing functionality on data packets at the level of a virtual local area network (VLAN). *See e.g.*, Ex. 1005, Abstract; Ex. 2010, ¶68. Petitioner's Ground 3 depends on incorporating Ke's multi-domain "virtual systems" into Coss's multi-domain firewall systems. *See* Petition at 46-48. As explained below, Ke fails to cure the deficiency of Coss, and the proposed Coss-Ke combination relies on impermissible hindsight. Ex. 2010, ¶68.

First, Petitioner's reliance on Ke to teach the claimed "*defining a node*" simply fails because no such teaching is found in Ke, including even the concept of a "*node*" itself. Specifically, in an attempt to cure the deficiency of Coss, the Petitioner maps Ke's "configuring an Internet security system" in the Coss-Ke combination to the "*defining a node*" claim limitation. *See* Petition at 46. However, similar to Coss which supports multiple domains, Ke's "configuration of the Internet security system" is also directed to supporting multiple ***domains*** (e.g., VLAN1, VLAN2) and focuses on "dynamic resource allocation" between different virtual private networks. *Compare* Ex. 1004, 3:36-4:3 ("Support for Multiple Security Domains") *with* Ex. 1005, ¶¶[0041] ("the inventive Internet security system provides dynamic resource allocation on a [sic] as needed basis for the different virtual private networks and associated systems"), [0059]-[0082]; *see also* Petition at 49 ("Both Coss and Ke are in the same field of art…protecting ***multi-domain systems*** with different firewall policies.") (emphasis added). As shown in Fig. 2 of Ke, the virtual local area networks ("VLANs") and "VLAN trunk (220) that carries all packets" are located "[o]n the secure side of the firewall device (210)." Ex. 1005, ¶[0033]. Nowhere does Ke teach "moving" devices (e.g., VLANs) between nodes to change their behavior or modeling the behavior of services and devices, as the '282 patent describes. Ex. 2010, ¶69.

As Dr. Franz explains, even if a POSITA would find themselves in simultaneous possession of both Coss and Ke, they would still not discover, anticipate, or find obvious the concept of a "*node*" as taught in the '282 patent, nor would it have been obvious how to combine these references without undue experimentation. *Id*. Accordingly, at a minimum, Coss in view of Ke does not disclose, teach, suggest, or render obvious the concept of "*defining a node*" at least because neither Coss or Ke discloses, teaches, suggests, or renders obvious the concept of a "*node*."

Second, Coss and Ke have different architectures, but neither of them individually or in combination teaches an "automated system [that] can automatically produce the requisite, specific firewall configuration" based on a firewall owner's general description of how the firewall should behave ('282 patent, 2:50-54) by modeling the behavior of services and devices using "*nodes*." Ex. 2010, ¶70. The Coss-Ke combination still fails to teach or suggest such system as described by the '282 patent.

Third, the Petitioner identifies no specific problem in Coss that a POSITA would have solved by importing Ke's VLAN-based virtual systems. *See e.g.*, Petition at 46-51. Coss does not mention VLANs, trunks, virtual interfaces, or a need for implementing such features, since Coss already achieves domain selection through the domain support engine (DSE) and per-domain tables. Ex. 1004, 1:61-

2:6; 6:3-65; 7:10-15. Additionally, the Petition alleges that "a POSITA would have recognized the benefits of adding additional runtime flexibility" in Ke, but apart from its general assertions such as "benefits in scalability and cost," the Petition does not explain what the purported "additional runtime flexibility" entails. Petition at 50. Petitioner's expert declaration tellingly repeats this almost verbatim and adds nothing further. *See* Ex. 1003, ¶154. The Petition also concedes that Coss currently uses "dynamic rules loaded and removed at runtime," and indeed, Coss's already has the purported "runtime flexibility" when its "[d]ynamic rules allow a given rule set to be ***modified based on events happening in the network*** without requiring that the entire rule set be reloaded." Ex. 1004, 8:38-40 (emphasis added). Therefore, the Petition's "complementary" argument (Petition at 50-51) is a result-oriented hindsight analysis, not an articulated reason to combine.

Accordingly, the proposed Coss-Ke combination in Ground 3 fails at least because Ke does not cure the deficiencies of Coss and the combination lacks a technically-grounded motivation to combine with a reasonable expectation of success.

V. GROUNDS 1 AND 2 FAIL TO DELINEATE BETWEEN § 102 AND § 103 AND FAIL TO PROPERLY ASSERT EITHER CATEGORY

Grounds 1 and 2 of the Petition rely on anticipation under 35 U.S.C. § 102 and obviousness under § 103, respectively, but are presented together in a manner

that obscures and inadequately develops either theory, particularly with respect to Claims 1 and 5 of the '282 patent. *See* Petition at 10 ("A. Grounds 1 and 2 – Claims 1-35 Are Anticipated by And At Minimum Obvious Over Coss"). Due to this lack of clarity, the grounds of the Petition are substantively deficient and noncompliant with 35 U.S.C. § 312(a)(3)[1] and the Board should deny institution.

As a preliminary matter, for numerous claim limitations, the Petition is unclear whether it asserts anticipation under § 102, obviousness under § 103, or both. Within this blended theory, it impermissibly collapses anticipation and obviousness, shifting between the two across the same parsed claim elements without coherent analysis. The result is not a principled application of either standard but a diffuse argument that obscures, rather than addresses, the dispositive deficiencies in the prior art.

The Petition's treatment of claim limitation 1[a] illustrates this defect. It

[1] 35 U.S. Code § 312(a) "Requirements of Petition.—A petition filed under section 311 ***may be considered only if***— . . . (3) the petition identifies, in writing ***and with particularity***, each claim challenged, ***the grounds on which the challenge to each claim is based***, and the evidence that supports the grounds for the challenge to each claim, ..." (emphasis added).

asserts that a POSITA "would have understood and at minimum found obvious" that applying access rules to packets "based on the domains ***necessarily*** requires" associating distinct rule sets with the corresponding domains. Petition at 18, (emphasis added). That is not anticipation. It is conjecture presented as obviousness and not associated with any affirmative disclosure in Coss. The Petition never shows that Coss discloses the claimed association of rule sets to domains. A POSITA gloss cannot substitute for a missing disclosure, and the Petition's ipse dixit about what is "necessary" does not cure the gap.

Claim 5 underscores the same overreach. Although the Petition purports to challenge Claim 5 on both anticipation and obviousness grounds (Petition at 3), it supplies no element-by-element mapping to Coss and identifies no objective disclosure in Coss. Instead, it relies entirely on what a POSITA supposedly "would have understood," and nothing more. Petition at 30. That is insufficient under either statutory provision.

Petitioner cannot have it both ways. If it proceeds on anticipation, it must identify where Coss discloses **each and every element and limitation** of the challenged claim. It does not. That failure is dispositive under § 102, and the anticipation theory collapses at the threshold. If instead Petitioner proceeds on obviousness, it must do far more than gesture at the prior art. It must demonstrate a clear teaching, suggestion, or motivation, or provide a reasonable explanation for

every claimed feature not explicitly or inherently described in the art, and supply a coherent rationale explaining why a POSITA would have combined those teachings to arrive at the claimed invention with a reasonable expectation of success. Petitioner does neither. Its obviousness case is devoid of a feature-by-feature showing and untethered to the factors articulated in *Graham v. John Deere Co.*, 383 U.S. 1 (1966) and reiterated in *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007). The court has "repeatedly emphasized that an obviousness inquiry requires examination of all four *Graham* factors and that an obviousness determination can be made only after consideration of each factor." *Nike, Inc. v. Adidas AG*, 812 F.3d 1326, 1335 (Fed. Cir. 2016). Here, for every claim element of the challenged claims, the Petition lacks any articulation of the second *Graham* factor (ascertaining the differences between the claimed invention and the prior art). While arguing such differences risks undercutting one's anticipation arguments, Petitioner in this case chose to avoid taking the risk at the expense of ignoring the legal standard of obviousness.

The improper ground not only requires Patent Owner to respond to multiple incomplete arguments but also would impel the Board, if the Petition is instituted, to analyze multiple unarticulated invalidity grounds under multiple legal standards. Furthermore, gaps in Petitioner's claim mapping (discussed briefly above) raise doubts that any § 102 argument was made in good faith. Yet Patent Owner is forced

to respond to both anticipation and obviousness arguments, despite neither theory being sufficiently explained for Patent Owner to appropriately rebut. Petitioner has improperly shifted the burden to the Board and to Patent Owner, and the Board should deny institution.

VI. PETITIONER IMPROPERLY RELIES ON POSITA'S KNOWLEDGE INSTEAD OF DISCLOSURE OR TEACHING IN THE PRIOR ART REFERENCE.

On July 31, 2025, the Director's office issued a memorandum (the "July Memorandum") putting all practitioners on notice that the Office "will enforce and no longer waive the requirement of 37 C.F.R. § 42.104(b)(4) (Rule 104(b)(4)) that a petition for inter partes review (IPR) "must specify where each element of the claim is found in the prior art patents or printed publications relied upon"" and prohibiting reliance on "applicant admitted prior art (AAPA), expert testimony, common sense, and other evidence that is not "prior art consisting of patents or printed publications" … to supply a missing claim limitation." July Memorandum at 1. The July Memorandum makes clear that reliance on a "general knowledge," such as by a POSITA, to fill in missing claim limitations from prior art reference(s) was impermissible and is limited to supporting motivation to combine and demonstrating the knowledge of a POSITA. *Id*. at 1-2. This change applies to any petition filed on or after September 1, 2025 (*id*. at 3) and, thus, applies to the instant Petition.

Petitioner disregarded the Director's instructions, and in direct contradiction to 35 U.S.C. §311(b)[2], by impermissibly relies on the knowledge of a POSITA to substitute for missing '282 patent claim limitations in the cited references, namely Coss. Particularly, the Petition fails to show that Coss discloses, teaches, or suggests multiple claim elements and limitations.

In Claim limitation [1C], Petitioner cherry-picks language from Coss about an IP packet "received by the firewall" that "supports multiple domains," and then impermissibly maps "firewall" to "domain" to meet the claim's requirement of "*receiving a packet at a first node of the at least one node*." Confronted with the obvious disconnect between a firewall and a domain, Petitioner attempts to paper over the gap with a generic POSITA gloss—asserting that a POSITA "would have understood" this "necessarily requires receiving the packet at the domain." Petition at 18–19 (citing Ex. 1003 ¶ 74). But the cited declaration completely omits any

[2] 35 U.S.C. § 311(b): "A petitioner in an inter partes review may request to cancel as unpatentable 1 or more claims of a patent ***only on a ground that could be raised under section 102 or 103 and only on the basis of prior art consisting of patents or printed publications***" (emphasis added).

discussion on such POSITA "understanding," and offers no citation to Coss—or any other evidence—supporting this argument. *Id*.

Returning to Claim 5, Petitioner's arguments rest solely on POSITA's knowledge by arguing that "POSITA would have understood that two sets of rules are necessarily either the same, or at least partially (if not completely) different" and based on that unsupported logic, concludes that Coss's first and second sets of firewall rules are "at least partially different." Petition at 30. The Petition provides no disclosure in Coss, no contemporaneous technical teaching, and no expert analysis tethered to the record demonstrating any actual differences between the purported "first" and "second" rule sets. The expert's declaration is near-verbatim recitation of the Petition, offering no independent analysis or substantive expertise. *Compare* Petition at 30, *with* Ex. 1003, ¶¶84-85.

The July Memorandum was clear that failures like this cannot be covered up by reliance on a POSITA knowledge. Petitioner's disregard for Rule 104(b)(4) provides a compelling reason for the Director to deny institution.

VII. CONCLUSION

For the reasons discussed above, Patent Owner respectfully requests that the Board deny Petitioner's Petition for *Inter Partes* Review of the '282 patent.

Dated: January 20, 2026

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel
Babak Tehranchi, Reg. No. 55,937

Back-Up Counsel
Yuanfeng Gao, Reg. No. 79,573
Kyle Canavera, Reg. No. 72,167
Thomas Millikan, Reg. No. 72,316
Ashlee Sherman, (To be admitted – Pro Hac Vice)

PERKINS COIE LLP
11452 El Camino Real, Ste. 300
San Diego, CA 92130

Attorneys for Netskope, Inc.

CERTIFICATE OF WORD COUNT UNDER 37 CFR § 42.24(d)

Under 37 C.F.R. § 42.24(d), the undersigned certifies that the word count for this Patent Owner's Preliminary Response to the Petition for *inter partes* review totals 6,159 words, excluding the parts exempted by 37 C.F.R. § 42.24(a). The word count was made using the built-in word count function in the Microsoft® Word software used to prepare this document.

Dated: January 20, 2026

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel
Babak Tehranchi, Reg. No. 55,937

Back-Up Counsel
Yuanfeng Gao, Reg. No. 79,573
Kyle Canavera, Reg. No. 72,167
Thomas Millikan, Reg. No. 72,316
Ashlee Sherman, (To be admitted – Pro Hac Vice)

PERKINS COIE LLP
11452 El Camino Real, Ste. 300
San Diego, CA 92130

Attorneys for Netskope, Inc.

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that I caused to be served a true and correct copy of the foregoing PATENT OWNER'S PRELIMINARY RESPONSE and accompanying exhibit by email to the electronic service addresses for Petitioner on the date indicated below:

Andrew D. Gish (Reg. # 67,562)
andrew@gishpllc.com
Ryan Iwahashi (Reg. # 63,378)
ryan@gishpllc.com

Dated: January 20, 2026

Respectfully submitted,

/Anita Chou/
Anita Chou
Patent Paralegal

PERKINS COIE LLP
1888 Century Park East, 17th Floor
Los Angeles, CA 90067