10 大 SASE 提供商应当提供的能力

在理想情况下，过渡到 SASE 架构其实很容易，只需按下一个按钮，就可以将整个网络架构迁移到梦幻般安全的云环境中。但很遗憾，在现实世界中并不会如此完美。不过，过度到 SASA 也不至于复杂到让人无所适从。

想要顺利过渡到 SASE 架构，首先得找到能胜任这项任务的提供商。SASE 提供商首先应帮助您利用现有投资，然后依托丰富的经验帮助您以最适合您业务的节奏无缝、安全地过渡到云交付的安全性。

1 统一的策略管理

通过单一界面从云端统管任何位置、本地和云端的安全性。

统一的策略管理必须确保随时随地以符合用户、设备和应用需求的策略提供安全的用户体验。

2 快速有效地防范高级威胁

防范不可见和未知的威胁，即便这些威胁已经过加密。

找到基于云的服务，利用这种服务执行静态和动态恶意软件检测，在检测到最复杂和最隐匿的威胁时瞬间识别威胁类型，并以近乎实时的速度进行拦截。

3 弹性和可扩展性

轻松有效地扩展物理、虚拟和基于云的安全环境。

您需要至简运维和大规模的安全性，这对最终用户来说是不可见的，并且绝对不能对用户体验产生负面影响。

4 采用单一策略框架的单一堆栈架构

利用现有投资作为关键业务云安全服务的入口。

一次性创建多个策略，然后利用统一的策略管理功能将其应用到任意位置，其中包括用户和基于应用的访问、IPS、反恶意软件，以及单一策略下的安全 Web 接入。

5 为分散的员工提供一致的安全性

让远程员工能够安全地访问高效办公所需的应用和资源。

一致的安全策略必须可以追踪用户、设备和应用，无需复制或重新创建规则集。

6 支持混合环境

对于 SASE 提供商来说，无论您的基础架构是在本地、云端还是混合环境中，都应全盘支持。

SASE 提供商必须能够帮助您无缝、安全地过渡到 SASE 架构，并以最适合您业务的节奏进行过渡。

7 单一身份来源

可以与市场上的所有身份解决方案提供商无缝集成。

SASE 提供商必须允许您选择最能满足您业务需求的身份提供商，而不是最适合他们的身份提供商。

8 动态用户细分

确保用户随时随地得到保护。

整合跟随用户的策略，并且通过精细化策略提供基于风险的自动访问控制，将第三方访问锁定为攻击媒介。轻松应对第三方访问，进一步减少边缘的攻击面。

9 经验证的安全防护效力

先做调查，找到一家能够提供高效安全防护的 SASE 提供商。

SASE 提供商必须展现出有效防范威胁（包括客户端和服务器端漏洞利用、勒索软件、僵尸网络和 DNS 隧道）的能力。提供商必须正面应对威胁环境的挑战，在您的本地环境和云端阻止攻击，并且必须以服务形式交付。

10 按您自己的节奏无缝过渡到云交付的安全性

在您做好准备之前，不应有人强迫您迁移至 SASE 架构。

通过统一的策略和直观的部署向导，在同一管理 UI 内按照自己的节奏无缝过渡到云交付的安全架构。无论策略服务位于何处，都可以轻松有效地编排、配置和管理这些服务。

11 附加优势：安全保证

自信满满地进行策略规则变更，确保策略变更富有成效。

无论是传统防火墙策略的规则，还是以服务形式交付的策略规则，都必须按照适当的顺序部署，以便发挥效用。SASE 提供商必须能够帮助您的 IT 团队理解这些规则集，并且自动标示重复和隐藏的规则，然后再实施。

每一次 SASE 迁移对您和您的组织来说都是独一无二的，但最终还是由您来选择如何设计、构建和维护这一新架构，以便在需要时优化所需的用户体验、服务和数据。无论您选择何种途径，最重要的是有一家提供商能够出现在您的面前，与您同舟共济，帮助您实施 SASE。

公司和销售总部

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

电话：888.JUNIPER (888.586.4737)

或 +1.408.745.2000

传真：+1.408.745.2100

www.juniper.net

亚太地区及欧洲、中东和非洲地区总部

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

电话：+31.0.207.125.700

传真：+31.0.207.125.701

JUNIPER NETWORKS | Driven by Experience™

文件编号：3050168

10 大 SASE 提供商应当提供的能力

在理想情况下，过渡到 SASE 架构其实很容易，只需按下一个按钮，就可以将整个网络架构迁移到梦幻般安全的云环境中。但很遗憾，在现实世界中并不会如此完美。不过，过度到 SASA 也不至于复杂到让人无所适从。

想要顺利过渡到 SASE 架构，首先得找到能胜任这项任务的提供商。SASE 提供商首先应帮助您利用现有投资，然后依托丰富的经验帮助您以最适合您业务的节奏无缝、安全地过渡到云交付的安全性。

1 统一的策略管理

通过单一界面从云端统管任何位置、本地和云端的安全性。

统一的策略管理必须确保随时随地以符合用户、设备和应用需求的策略提供安全的用户体验。

2 快速有效地防范高级威胁

防范不可见和未知的威胁，即便这些威胁已经过加密。

找到基于云的服务，利用这种服务执行静态和动态恶意软件检测，在检测到最复杂和最隐匿的威胁时瞬间识别威胁类型，并以近乎实时的速度进行拦截。

3 弹性和可扩展性

轻松有效地扩展物理、虚拟和基于云的安全环境。

您需要至简运维和大规模的安全性，这对最终用户来说是不可见的，并且绝对不能对用户体验产生负面影响。

4 采用单一策略框架的单一堆栈架构

利用现有投资作为关键业务云安全服务的入口。

一次性创建多个策略，然后利用统一的策略管理功能将其应用到任意位置，其中包括用户和基于应用的访问、IPS、反恶意软件，以及单一策略下的安全 Web 接入。

5 为分散的员工提供一致的安全性

让远程员工能够安全地访问高效办公所需的应用和资源。

一致的安全策略必须可以追踪用户、设备和应用，无需复制或重新创建规则集。

6 支持混合环境

对于 SASE 提供商来说，无论您的基础架构是在本地、云端还是混合环境中，都应全盘支持。

SASE 提供商必须能够帮助您无缝、安全地过渡到 SASE 架构，并以最适合您业务的节奏进行过渡。

7 单一身份来源

可以与市场上的所有身份解决方案提供商无缝集成。

SASE 提供商必须允许您选择最能满足您业务需求的身份提供商，而不是最适合他们的身份提供商。

8 动态用户细分

确保用户随时随地得到保护。

整合跟随用户的策略，并且通过精细化策略提供基于风险的自动访问控制，将第三方访问锁定为攻击媒介。轻松应对第三方访问，进一步减少边缘的攻击面。

9 经验证的安全防护效力

先做调查，找到一家能够提供高效安全防护的 SASE 提供商。

SASE 提供商必须展现出有效防范威胁（包括客户端和服务器端漏洞利用、勒索软件、僵尸网络和 DNS 隧道）的能力。提供商必须正面应对威胁环境的挑战，在您的本地环境和云端阻止攻击，并且必须以服务形式交付。

10 按您自己的节奏无缝过渡到云交付的安全性

在您做好准备之前，不应有人强迫您迁移至 SASE 架构。

通过统一的策略和直观的部署向导，在同一管理 UI 内按照自己的节奏无缝过渡到云交付的安全架构。无论策略服务位于何处，都可以轻松有效地编排、配置和管理这些服务。

11 附加优势：安全保证

自信满满地进行策略规则变更，确保策略变更富有成效。

无论是传统防火墙策略的规则，还是以服务形式交付的策略规则，都必须按照适当的顺序部署，以便发挥效用。SASE 提供商必须能够帮助您的 IT 团队理解这些规则集，并且自动标示重复和隐藏的规则，然后再实施。

每一次 SASE 迁移对您和您的组织来说都是独一无二的，但最终还是由您来选择如何设计、构建和维护这一新架构，以便在需要时优化所需的用户体验、服务和数据。无论您选择何种途径，最重要的是有一家提供商能够出现在您的面前，与您同舟共济，帮助您实施 SASE。

公司和销售总部

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

电话：888.JUNIPER (888.586.4737)

或 +1.408.745.2000

传真：+1.408.745.2100

www.juniper.net

亚太地区及欧洲、中东和非洲地区总部

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

电话：+31.0.207.125.700

传真：+31.0.207.125.701

Driven by Experience™

3050168-001-ZH 2023 年 8 月