阿姆瑞特虚拟安全网关（VSG）

阿姆瑞特虚拟安全网关（VSG）系列是专为需要高级别安全性的虚拟化和云计算环境而设计的专业的下一代安全网关，可以无缝的运行在VMware、Hyper-V、Citrix或KVM内核的虚拟化平台上。VSG内部集成了防火墙、抗DoS/DDoS攻击、网络扫描保护、接入安全、僵尸网络阻止、地理IP拦截等先进 网络安全组件，可以为虚拟化或云计算环境提供全方位的网络安全，建立起与物理环境中相同功能，等同强度的立体安全屏障，保障虚拟网络安全。

功能&技术特点：

➢ 非凡的下一代安全网关功能

阿姆瑞特虚拟安全网关能够提供超大的并发连接数，支持静态路由、OSPF、路由负载均衡、服务器负载均衡、链路监视、Server VLAN 等高级网络功能，并具有强大的抗 DoS/DDoS 攻击、僵尸网络阻止、IP 欺骗阻止等特性，通过与其强大的网络行为攻击识别和阻止以及精细的应用控制的组合，能够为用户提供从网络层到应用层的完美保护。

➢ 灵活的网络接入功能

作为一款虚拟化网络基础设备 ,阿姆瑞特虚拟安全网关配置了多种网络接口 ,可以以路由、透明、混合的模式部署于任何形式的网络拓扑中，同时支持 IPv4、IPv6 以及 6 in 4 管道，其强大的 NAT 和服务器映射功能使用户可以轻松地将其部署于 IDC 网络出口处，同时也可因 DHCP 和 DHCPv6、用户认证等功能而被部署于网络的接入部位，实行虚拟机接入安全管理。

➢ 细粒度的访问控制功能

除了传统的基于 IP 地址、端口的访问控制以外 ,阿姆瑞特虚拟安全网关还支持基于应用、URL、Web 内容、文件类型、地理 IP 等的访问控制。通过访问控制功能，阿姆瑞特虚拟安全网关甚至可以控制 FTP、SMTP 等一些应用协议中的命令，以防止因攻击者获得权限而恶意删除文件或暴露用户名和口令。

➢ 强大的攻击抵御能力

阿姆瑞特虚拟安全网关可以抵抗多种形式的攻击 ,包括 Syn-flood、Land-Based、UDP Flood、Ping Flood、Ping of Death、Tear Drop 等，并且这些攻击除 Syn-flood 外都无需配置，设备自动识别并加以阻止。

地理 IP 控制功能

针对来自于一个国家或地区的攻击，网络管理员无需收集并维护攻击者的源 IP，只需在阿姆瑞特虚拟安全网关的管理页面中选择相应的国家或地区，就可以轻松阻止来自或去往这些国家或地区的流量，也可以对其流量设置带宽限制。

IP 名声评分功能

阿姆瑞特维护着一个 IP 名声数据库，这个数据库实时地对全球所有的 IP 地址进行评分，凡是僵尸主机、僵尸主机的主控端、各种攻击的源 IP 都会具有较低（差）的名声值，因此，管理人员可以通过这一技术来轻松达到高效阻止攻击源的目的。

服务器负载均衡

单独的一台虚拟服务器在访问量过大的时候会出现响应速度慢，甚至连接无法建立等情况，从而出现与受到 DoS 攻击类似的现象。为了更好地服务于特定时间段内访问量激增的情况，阿姆瑞特虚拟安全网关提供了服务器负载均衡功能，可以深入服务器本身以了解各服务器详细的资源使用情况和实时负载情况，以此来决定向每台服务器分发多少连接。

应用控制功能

阿姆瑞特虚拟安全网关支持应用控制功能，它采用的特征码，可以精确识别上千种应用和协议及其子应用和协议，比如可以允许仅通过 Skype 发送即时消息，而不允许传输文件。这种应用控制的模式，可以在保证通信的同时防止机密文件被传播，更加突出了阿姆瑞特在为用户提供便利性的基础上仍能保证信息安全的服务理念。

跨平台统一威胁管理

阿姆瑞特虚拟安全网关作为专门针对虚拟化和云计算环境而设计的下一代安全网关，采用跨平台通用架构设计，可以无缝部署在所有主流虚拟化平台之中。阿姆瑞特独有的非通用操作系统安全内核，在提供强大安全防护功能的同时，更提供超高的吞吐量。无论是 VMware 或 Citrix，Hyper-V 还是 KVM，阿姆瑞特虚拟安全网关都可与阿姆瑞特物理下一代安全网关协同工作，提供跨平台统一威胁管理功能。

丰富的路由功能

阿姆瑞特虚拟安全网关具有强大的路由功能，可以被部署在 IDC 出口对内部虚拟提供 NAT 和服务映射，或者部署于虚拟网络内部以纯路由模式为不同业务分区提供访问隔离。同时也可以被透明地部署于需要保护的资源前面以实现无感知安全防护。

HTTPS 终结

当前有不少 WEB 服务器仍然在提供 HTTP 而非更安全的 HTTPS 服务，甚至一些重要的表单也没有使用 HTTPS 协议，这是一个极大的安全威胁。阿姆瑞特虚拟安全网关所提供的 https 终结功能可以轻松把原有的 http 页面转换成 https 页面，从而消除这一威胁。

➢ 链路监视与路由备份

任何一个虚拟化平台都具有多条物理上行链路，阿姆瑞特虚拟安全网关可以监视链路连接的状态、网关设备的活动性以及远程主机的响应速度，不仅可以在链路完全断开的情况下自动切换，而且还可以在某条链路质量较差的时候把连接切换到其它线路上。

➢ 网络扫描保护

网络扫描是黑客发起攻击的第一个步骤，他们在外部的主机上运行软件以进行第一步的侦察，通过这些方法就可以得到关于 IP、端口号以及域名等信息，甚至对目标主机进行暴力破解。阿姆瑞特虚拟安全网关能够识别这些扫描行为，丢弃扫描连接并把黑客的 IP 地址记入黑名单。

➢ IPv6 Ready

阿姆瑞特虚拟安全网关已获得了 IPv6 Ready 的认证，以双栈和隧道的方式全面支持 IPv6，不仅能够基于 IPv6 的 IP 地址等信息来进行访问控制，更可以支持 6 in 4 通道，其产品中有丰富的 IPv6 功能特性集，包括 DHCPv6、DNSv6 客户端、IPv4 路由和 IPv6 路由的共存。

➢ 服务 VLAN

网络扁平化是近年来网络发展的一个新趋势，有不少规模较大的网络都在这一方面进行了一定程度的尝试，阿姆瑞特虚拟安全网关通过支持符合 IEEE 802.1ad 标准的 Service VLAN（服务 VLAN 或 Q-in-Q VLAN）来为用户提供网络扁平化的技术基础。这一技术通过把传统的 VLAN 再封包的方法来解决传统 VLAN 在跨网络传输时的 VLAN ID 冲突问题，并为网络扁平化提供有力的技术支持。同时，与 MPLS 相比，服务 VLAN 也可以帮助用户建立起互联的专有网络，而成本却比 MPLS 低得多。

➢ 链路聚合

为了提供更大的吞吐量和更高的带宽，阿姆瑞特虚拟安全网关产品使用整机状态表的方式，使虚拟安全网关支持端口聚合成为了可能。端口聚合技术将多物理接口当作一个单一的逻辑接口来处理，它允许与交换机之间通过多个端口并行连接同时传输数据以提供更高的带宽，有效地提高设备间的传输速度，从而消除网络访问中的瓶颈。

➢ 集中管理与日志分析

阿姆瑞特提供了一个名为 InControl 的统一威胁管理平台。用户可以使用 InControl 平台对虚拟安全网关和物理安全网关进行统一的管理，并直观地以各种图表来自定义设备的状态、性能监视页面，并对设备配置进行实时备份、更改、配置差异分析。同时 InControl 可以搜集详细的日志数据，并可通过强大的逻辑查询功能对数据进行分析，深度了解用户的网络行为,并进行流量统计、访问统计，并展现潜在安全威胁等等。阿姆瑞特 InControl 向用户提供基于 WCF 的 SDK，用户通过调用 API 就可以开发出具有自己特色的集中管理工具。

产品参数

产品型号	AM-V2	AM-V3	AM-V5	AM-V7	AM-V9	AM-V10
吞吐量	0.3 Gbps	1 Gbps	2 Gbps	3 Gbps	6 Gbps	10 Gbps
并发连接数	16,000	64,000	128,000	250,000	512,000	2,000,000
以太网接口	可升到 3 个	可升到 4 个	可升到 6 个	可升到 8 个	可升到 10 个	可升到 10 个
虚拟接口 (VLAN)	8	32	256	512	1,024	2,048
虚拟路由器	5	25	50	100	200	1,024
外形	软件					

* 吞吐量性能基于RFC 2544。实际性能取决于网络条件、激活服务和主机的硬件功能。

全国分支机构

北京（总部）
地址：北京市朝阳区清河营东路中铁国际城•乐想汇2号楼720室
电话：(010)84476440

西安办事处
地址：西安市经开区迎宾大道138号豪盛花园D2501室
电话：(029)88855367

成都办事处
地址：成都市锦江区锦华路一段8号万达锦华城7单元1201号
电话：(028)84191711

上海办事处
地址：上海市青浦区华徐公路962弄69号复能大厦405室
电话：(021)62676906

南京办事处
地址 :南京市鼓楼区集庆门大街268号苏宁慧谷E2座1613室
电话：(025)85652586

重庆办事处
地址：重庆市九龙坡区万象大道华润中心28栋1708室
电话：(023) 88959717

广州办事处
地址：广州市天河区中山大道中393号天长商贸园B209
电话：(020)87584690

郑州办事处
地址：郑州市惠济区新城路睿谷创新中心3区5号楼401室
电话：(0371)55958385

昆明办事处
地址：昆明市官渡区矣六街道万科魅力之城A1-6-2909
电话：(0871)67202231

北京云安信息技术有限公司
咨询热线：400-8060-389
www.amaranten.cn
www.bjyunan.cn

官方微信　　官方网站