- Prerequisites

Prerequisites

Umbrella Package Requirements

- You must be licensed for either DNS Security Essentials, DNS Security Advantage, Insights, or Platform. For more information, see Umbrella Package Comparison.

Virtual Appliance Requirements

- **Two virtual appliances (VAs) per Umbrella site**—VAs must be deployed in pairs to ensure redundancy at the DNS level and to allow for updates without downtime.
- **VA Specifications**—At a minimum, each VA requires the following allocated resources:
    - One virtual CPU
    - Minimum 512MB of RAM (1GB RAM recommended)
    - 7GB of disk space.

Each VA is able to process millions of DNS requests per day using these specifications. If you believe your network will exceed this number, see Appendix B – Sizing Guide.

> □ **Important**
>
> High-traffic site VAs should use two virtual CPUs and 2048MB of RAM per VA.
> A high-traffic site is one that has more than 500 DNS queries per second coming from the overall network.

- **Correct Date/Time**—Ensure your hypervisor host has the correct date and time. The incorrect date or time can cause update or sync issues with the VAs. The VA syncs time independently and is always set to UTC.

VMware Requirements

- VMware ESX or ESXi (supported versions as per VMware)
- VMware Cloud on AWS

Microsoft Hyper-V Requirements

One of the following Windows Server operating systems:

- Windows 2008 R2 Server with Hyper-V role
- Hyper-V Server 2008

- Windows Server 2012, SP1, or R2 (Standard or Datacenter) or 2016 with Hyper-V role
- Hyper-V Server 2012 or 2012 R2 or 2016

Note: Deploying the virtual appliance through System Center Virtual Machine Manager (SCVMM) has not been qualified and is not officially supported.

Cloud Platform Requirements

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

KVM Requirements

- KVM on Ubuntu Linux (supported LTS versions)
- KVM on Red Hat Linux (supported versions)

Networking Requirements

Once VAs are deployed and ready to be utilized, endpoint clients must exclusively resolve DNS through the VAs and not your local DNS forwarders. This is usually accomplished through the network's DHCP configuration. For more information, see Local DNS Forwarding.

The following firewall/ACL requirements ensure VAs can communicate with the Umbrella cloud services and local DNS forwarders/servers. These requirements apply to both VMWare and Hyper-V deployments.

Port and Protocol	Destination	Note
53 TCP + UDP	• 208.67.220.220/32 • 208.67.222.222/32 • 208.67.222.220/32 • 208.67.220.222/32 *Your DNS Forwarder IPs*	**Standard and Encrypted DNS**—If utilizing a default deny firewall ruleset for local traffic, add the internal IP addresses of any local DNS forwarders/servers to the firewall ruleset, so that the VAs forward local queries accordingly. Note that these ports are used to establish DNSCrypt. For more information, see DNScrypt.
443 TCP + UDP	• 67.215.92.0/24 • 67.215.71.201/32 • ocsp.digicert.com • crl4.digicert.com • 208.67.220.220/32 • 208.67.222.222/32 • 208.67.220.222/32 • 208.67.222.220/32 • 146.112.255.155	**HTTPS**—Used for registration, health checks, and updates from Umbrella. ocsp.digicert.com and crl4.digicert.com use a CDN and are not assigned static IP addresses, thus are subject to change. Currently, these domains resolve to the following IPs: • 72.21.91.29 • 117.18.237.29 • 93.184.220.29 • 205.234.175.175 In addition, 443 is used as failover for DNSCrypt if 53 is unavailable and talks to 208.67.220.220 to probe. For more

		information, see DNSCrypt.
80 TCP	67.215.92.0/24 ocsp.digicert.com crl4.digicert.com	**HTTP**—Used for fetching the SSL revocation list to initiate the HTTPS connection.
123 UDP	91.189.94.4/32 91.189.89.199/32 91.189.91.157/32 91.189.89.198/32	**NTP**—Protocol to synchronize time.
443 TCP	disthost.opendns.com disthost.umbrella.com	Updates to the VA.
22 25 53 80 443 or 4766 TCP	s.tunnels.ironport.com	Required for the customer-initiated SSH support tunnel. For more information, see On-Demand Tech Support SSH Tunnel for Virtual Appliances.
5353 TCP + UDP	208.67.220.220/32 208.67.222.222/32	5353 is used as failover for DNSCrypt if 53 or 443 is unavailable. For more information, see DNSCrypt.
53 UDP + TCP	the VA(s)	Required for DNS to flow between client and VA. TCP optional.
443 TCP	the VA(s)	Required for Chromebook client trusted network feature.
443 TCP	the VA(s)	Used to send user/IP mapping (one-way) from the Active Directory (AD) connector to the VA.

SSH Support Tunnel

The tunnel must be established by the customer to the Cisco support team.
For more information, see On-Demand Tech Support SSH Tunnel for Virtual Appliances.

Networking: Additional Considerations

Intrusion Protection Systems (IPS) and Deep Packet Inspection (DPI)—If utilizing an IPS or DPI, ensure that traffic on port **53 TCP/UDP** to and from the VAs is excluded from packet inspection, as DNS Safeguard's DNS encryption methods might be flagged and dropped. If the VAs cannot successfully send and receive encrypted DNS packets, DNS Safeguard displays a warning in the dashboard.

Network Address Translation (NAT)—If a routing device running a separate NAT is placed between endpoints and VAs, an endpoint's IP address will show as the NAT device's IP address in the DNS Safeguard dashboard. The endpoints must reach the VAs without being subjected to a separate NAT. If you are unable to remove a routing device with a separate NAT, you may have to run a separate set of VAs within that NAT. If you have any questions regarding this matter, contact Support.

HTTP Proxies / Content Filtering—Most solutions attempting to locally proxy, cache, or filter HTTP/HTTPS traffic