FortiNAC

Production DNS Records for Agent Communication

Version: 8.x

Date: January 10, 2020

Rev: D

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM
http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET

Monday, September 10, 2018

Contents

Overview

Agent Server Discovery is a mechanism used by different types of agents to determine the identity of the FortiNAC Server or Application Server to which the agent should connect. Some agents use SRV and TXT records contained within both FortiNAC's DNS server and your production DNS server. The records used by the Agent for identifying and connecting to the FortiNAC server vary depending on the type of Agent used.

In addition to DNS records, the Persistent Agent (PA) can also obtain the server identity information using a software management program (such as a GPO Policy, Casper or Munki). If the configurations are not pushed via software, then SRV records on the corporate production DNS servers are required.

Note: For security purposes, it is recommended to use a software management program if possible. See **Persistent Agent Deployment and Configuration** in the Document Library.

Adding a DNS SRV Record Example

DNS servers will vary based on the operating system of the computer used to house them. The example below is for a DNS server running on a Windows operating system with the SRV records added from a command prompt. You may prefer to use another method to add records to your DNS Server.

1. On the Windows Desktop click **Start > Run**.
2. On the Run dialog in the **Open** field type **command** and click **OK**.
3. At the command prompt type the following:

   ```
   > dnscmd /RecordAdd yourdomain.com _bradfordagent._udp.yourdomain.com. SRV 0 0
   4567 servername.domainname.com.
   ```

4. To add the next record type the following:

   ```
   > dnscmd /RecordAdd yourdomain.com _bradfordagent._tcp.yourdomain.com. SRV 0 0
   4568 servername.domainname.com.
   ```

In the commands above yourdomain.com is the zone supplied via DHCP (Connection-specific DNS Suffix on a Windows station in "ipconfig /all" output). server-name.domainname.com is the FQDN of the FortiNAC Application Server or server that is running the captive portal. Note that there is a period (.) after .com at the end of the FQDNs and node names.

The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a High Availability environment.

Required Production DNS Server Records

From the DNS example in the section above you must include specific entries in your production DNS server. The examples below list each entry and provide notes about its function and the agents affected.

Dissolvable Agent 3.1 and Higher

Note: Production DNS records for the Dissolvable Agent are only required if the agent is being installed from production. Typically, the agent is being installed from an isolation network where FortiNAC acts as the DNS server.

```
_networksentry._tcp   PTR AgentConfig._networksentry._tcp
AgentConfig._networksentry._tcp SRV 0 0 443 servername.domainname.com.
                                    TXT path=/registration/agent/config
```

These lines work together to define the AgentConfig service. The first line indicates the name of the service and sets the type (_networksentry._tcp).

The second and third lines are the SRV record and indicate the FQDN of the server to which the agent will connect. 443 is the port and should not be changed. In the example, the name of the server is servername.domainname.com. This must match the name in the valid certificate used to secure the portal. Note that the period (.) at the end of servername.domainname.com. is required. The TXT line contains the path.

The agent uses the information contained in these entries to construct a URL for the server to which it should connect. Using the records shown above the agent would construct the following:

```
https://servername.domainname.com:443/registration/agent/config
```

Android Agent

```
_networksentry._tcp.discovery.portal.yourdomain.com SRV 0 0 443 servername
.domainname.com.
_networksentry._tcp.discovery.portal.yourdomain.com TXT path=/registration
/agent/config
```

These lines are the SRV record and indicate the FQDN of the server to which the agent will connect. They are the detailed version of the lines below that are included in the domain.zone.reg file. It is recommended that you use the detailed entry when editing your production DNS, however, either entry is acceptable.

```
_networksentry._tcp SRV 0 0 443 servername.domainname.com.
                        TXT path=/registration/agent/config
```

443 is the port and should not be changed. In the example, the name of the server is servername.domainname.com. This must match the name in the valid certificate used to secure the portal. Note that the period (.) at the end of server-name.domainname.com. is required. The TXT line contains the path.

The agent uses the information contained in these entries to construct a URL for the server to which it should connect. Using the records shown above the agent would construct the following:

```
https://servername.domainname.com:443/registration/agent/config
```

Persistent Agent

```
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 servername.domainname.com.
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 servername.domainname.com.
```

These SRV records indicate the FQDN of the server to which the agent will connect. 4567 and 4568 are the ports on which the server listens and should not be changed. In the example, the name of the server is servername.domainname. Note that the period (.) at the end of servername.domainname.com. is required.

This entry is used by the Persistent Agent. The Persistent Agent has other mechanisms for determining where its server is such as registry entries on the host or information contained in Persistent Agent Properties on the server. However, if those options are not available, the Persistent Agent does use DNS to locate a server. Refer to the Persistent Agent Deployment Configuration document in the Fortinet Document Library for details.

Persistent Agent in L2 or L3 HA Environment

In a High Availability environment (L2 or L3), SRV records must be added for all of the servers in order by priority. A priority of zero (0) takes highest precedence. If using L2 HA, only add the names of the physical servers (not the shared name).

The below example shows SRV records for the Primary Server with a priority of zero (0) and Secondary Server with a priority of one (1).

```
_bradfordagent._tcp.yourdomain.com   SRV  0 0 4568 primaryas.domainname.com.
_bradfordagent._udp.yourdomain.com   SRV  0 0 4567 primaryas.domainname.com.
_bradfordagent._tcp.yourdomain.com   SRV  1 0 4568 secondaryas.domainname.com.
_bradfordagent._udp.yourdomain.com   SRV  1 0 4567 secondaryas.domainname.com
```

When using the PA in a multiple FortiNAC Server environment, the best prac- tice is to set the registry keys via software push. If this is not possible, configure SRV records using the below guidelines.

Multiple FortiNAC Server Environment Requirements

Single Production DNS Server Shared By All FortiNAC Servers

No High Availability

Include all FortiNAC Server names with equal priority in the SRV records returned from the production DNS server.

The following shows DNS configuration entries for two FortiNAC configurations. These records are used by the Persistent Agent.

```
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 appserver1.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 appserver1.domainname.com.
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 appserver1.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 appserver1.domainname.com.
```

In the commands above yourdomain.com is the zone. appserver1.domainname.com and appserver2.domainname.com are the FQDNs of the FortiNAC Application Servers or servers that are running the captive portal. Note that there is a period (.) after .com. at the end of the FQDNs and node names.

FortiNAC Servers Configured for L2 High Availability

Include all FortiNAC Server (shared ip address) names with equal priority in the SRV records returned from the production DNS server.

The following shows DNS configuration entries for two FortiNAC configurations. These records are used by the Persistent Agent.

```
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 appserver1.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 appserver1.domainname.com.
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 appserver2.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 appserver2.domainname.com.
```

In the commands above yourdomain.com is the zone. appserver1.domainname.com and appserver2.domainname.com are the FQDNs of the FortiNAC Application Servers or servers that are running the captive portal. Note that there is a period (.) after .com. at the end of the FQDNs and node names.

FortiNAC Servers Configured for L3 High Availability

Add SRV records for all of the servers in order by priority. Priority is the first number after SRV in the example. Primary servers should take higher precedence (0).

These records are used by the Persistent Agent.

```
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 appserver1primaryas.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 appserver1primaryas.domainname.com.
_bradfordagent._tcp.yourdomain.com SRV 1 0 4568 appserver1secondaryas.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 1 0 4567 appserver1secondaryas.domainname.com.
_bradfordagent._tcp.yourdomain.com SRV 0 0 4568 appserver2primaryas.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 0 0 4567 appserver2primaryas.domainname.com.
_bradfordagent._tcp.yourdomain.com SRV 1 0 4568 appserver2secondaryas.domainname.com.
_bradfordagent._udp.yourdomain.com SRV 1 0 4567 appserver2secondaryas.domainname.com.
```

Separate Production DNS Server Per FortiNAC Server

Include the FortiNAC Server name in the SRV records returned from the production DNS server local to that FortiNAC Server. Use the entries for the stand- alone server as shown in the previous examples.

Verify

Once records are in place, confirm DNS server responds to SRV queries appropriately.

Using nslookup

yourdomain.com = the zone

Records for Persistent Agent:

```
nslookup -querytype=srv _bradfordagent._tcp.yourdomain.com
nslookup -querytype=srv _bradfordagent._udp.yourdomain.com
```

Records for Dissolvable Agent:

```
nslookup -querytype=srv _networksentry._tcp.yourdomain.com
nslookup -querytype=txt _networksentry._tcp.yourdomain.com
nslookup -querytype=srv AgentConfig._networksentry._tcp.yourdomain.com
nslookup -querytype=txt AgentConfig._networksentry._tcp.yourdomain.com
```

Records for Android Agent:

```
nslookup -querytype=srv _networksentry._tcp.discovery.portal.yourdomain.com
nslookup -querytype=txt _networksentry._tcp.discovery.portal.yourdomain.com
```

Example

Querying Records for Persistent Agent Using `nslookup` where Connection-specific DNS suffix (zone) is bradfordnetworks.com. An answer should return with the host name specified in the DNS record.

```
> nslookup -querytype=srv _bradfordagent._tcp.bradfordnetworks.com

Server:   DNSServer.bradfordnetworks.com
Address:   192.165.7.6
_bradfordagent._tcp.bradfordnetworks.com              SRV service location:
priority         = 0
weight           = 0
port             = 4568
svr hostname     = NetSen.bradfordnetworks.com
NetSen.bradfordnetworks.com       internet address = 192.165.8.5

> nslookup -querytype=srv _bradfordagent._udp.bradfordnetworks.com

Server:   DNSServer.bradfordnetworks.com
Address:   192.165.7.6
_bradfordagent._udp.bradfordnetworks.com              SRV service location:
priority         = 0
weight           = 0
port             = 4567
svr hostname     = NetSen.bradfordnetworks.com
NetSen.bradfordnetworks.com       internet address = 192.165.8.5
```

Using Domain Information Groper

Records for Persistent Agent:

```
dig SRV _bradfordagent._tcp.yourdomain.com
dig SRV _bradfordagent._udp.yourdomain.com
```

Records for Dissolvable Agent:

```
dig SRV _networksentry._tcp.yourdomain.com
dig TXT _networksentry._tcp.yourdomain.com
dig SRV AgentConfig._networksentry._tcp.yourdomain.com
dig TXT AgentConfig._networksentry._tcp.yourdomain.com
```

Records for Android Agent:

```
dig SRV _networksentry._tcp.discovery.portal.yourdomain.com
dig TXT _networksentry._tcp.discovery.portal.yourdomain.com
```

Example

Querying Records for Persistent Agent Using Domain Information Groper where Connection-specific DNS suffix (zone) is bradfordnetworks.com.

```
> dig SRV _bradfordagent._tcp.bradfordnetworks.com
; <<>> DiG 9.9.4-RedHat-9.9.4-18.el7 <<>> SRV _bradfordagent._tcp.bradfordnetworks.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31331
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;_bradfordagent._tcp.bradfordnetworks.com. IN SRV

;; ANSWER SECTION:
_bradfordagent._tcp.bradfordnetworks.com. 3600 IN SRV 0 0 4568 NetSen.bradfordnetworks
.com.

;; ADDITIONAL SECTION:
NetSen.bradfordnetworks.com. 3600 IN       A         192.165.8.5
;; Query time: 0 msec
;; SERVER: 192.165.7.6#53(192.165.7.6)
;; WHEN: Wed Jul 06 08:55:45 EDT 2016
;; MSG SIZE    rcvd: 134


> dig SRV _bradfordagent._udp.bradfordnetworks.com
; <<>> DiG 9.9.4-RedHat-9.9.4-18.el7 <<>> SRV _bradfordagent._udp.bradfordnetworks.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59914
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;_bradfordagent._udp.bradfordnetworks.com. IN SRV

;; ANSWER SECTION:
_bradfordagent._udp.bradfordnetworks.com. 3600 IN SRV 0 0 4567 NetSen.bradfordnetworks
.com.

;; ADDITIONAL SECTION:
NetSen.bradfordnetworks.com. 3600 IN       A        192.165.8.5

;; Query time: 0 msec
;; SERVER: 192.165.7.6#53(192.165.7.6)
;; WHEN: Wed Jul 06 08:52:13 EDT 2016
;; MSG SIZE    rcvd: 134
```