

Configuring of the Firewall Appliance ONE Network Access

Document Identifier: 00321

Version: 2.0



Ontario

eHealth Ontario

Copyright Notice

This document is copyright of eHealth Ontario (eHO).

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHO. The information contained in this document is proprietary to eHO and may not be used or disclosed except as expressly authorized in writing by eHO.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Revision History

Date	Version	Revision
July 2007	2.0	Modification for ONE Network Access Release 2 The title of this document has changed from <i>Configuration of SOFAs</i>
September 2005	1.0	Initial Release

Authorized Reader

This document is authorized to the following organizational roles:

- Role(s)** _____
- LAN installer

Table of Contents

1.0	About this Document	4
1.1	Document Approach and Scope	4
1.2	Audience.....	4
2.0	Definition of Site Types	5
3.0	Firewall Appliance Configuration Overview.....	6
3.1	Firewall Constraints	6
3.2	Out of Scope	6
3.3	Anti-virus.....	7
3.3.1	Web filtering.....	7
3.3.2	Access Controls	7
4.0	IP Address Configuration	8
4.1	Firewall ONE NETWORK Port.....	8
4.2	Support for Local DNS resolution	8
5.0	External Communications Configuration	9
5.1	eHO Standard Firewall Rules.....	9
5.2	Gateway-to-Gateway VPN Tunnels	9
6.0	Firewall Configuration Management	10
6.1	Change Request Definition and Scope.....	10
6.2	Included Services.....	10
7.0	Appendix A – Glossary.....	11

Table of Tables

N/A

Table of Figures

Figure 1 – Three Site Hub and Spoke Configuration	5
---	---

1.0 About this Document

1.1 *Document Approach and Scope*

Each ONE Network site is provided with a managed **Firewall Appliance**. This document describes the specifications for configuration of these Firewalls to support:

- Unique IP address range assigned by eHO to the LAN at each ONE Network site.
- Secure communication channels between each group of ONE Network Spoke sites and their Hub site.
- A system designed to defend against unauthorized access to or from a private network using specific firewall rules

1.2 *Audience*

This document is intended for:

- Technical planners, operational and support staff from eHO and the eHO ONE Network Vendor.
- Staff and vendors who support the computer systems of eHO ONE Network Subscribers.

2.0 Definition of Site Types

For OMAeS, eHO supports two standard configuration models.

- **Stand Alone** - A ONE Network site that does not require access to servers at another ONE Network site is called a Standalone Site. In terms of the Physician IT program, this would be used for a CMS ASP, CMS Local configuration 1, or CMS Local configuration 3 implementation.
- **Hub and Spoke** - Some eHO ONE Network Subscribers are members of a group that operate from several sites, where each site has a separate ONE Network connection. The group may operate a central server at one site for use by all group members. In such a case, the site with the server(s) is called the Hub Site, and a site that needs to access the server(s) are called a Spoke Site. In terms of the Physician IT program, this would be used for a CMS Local configuration 2 implementation. A three site Hub and Spoke configuration would look like this:

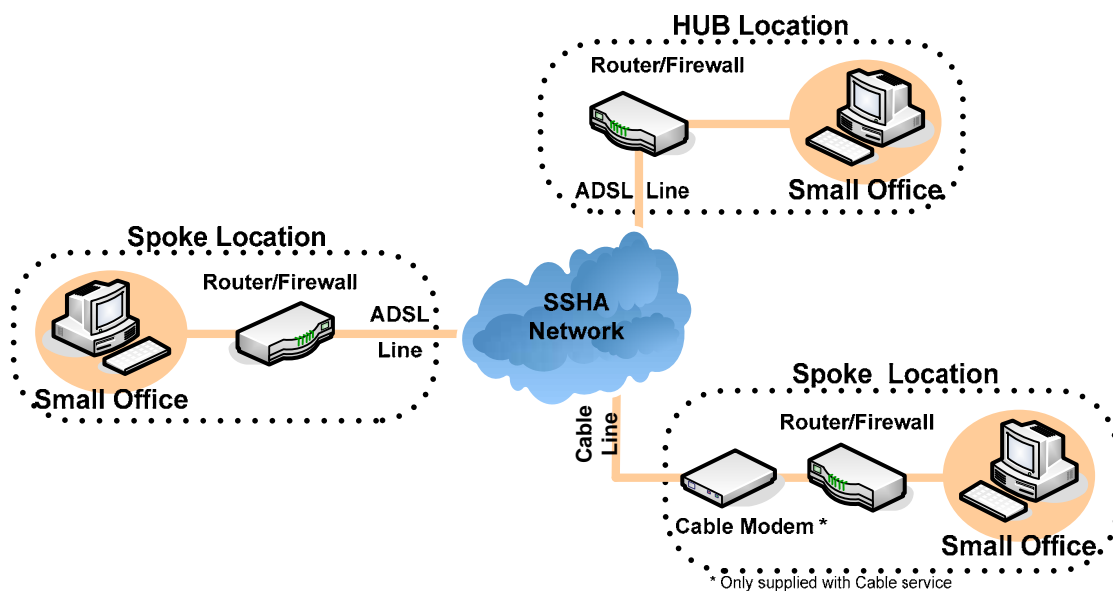


Figure 1 – Three Site Hub and Spoke Configuration

3.0 Firewall Appliance Configuration Overview

The following features and configuration parameters are assigned for all Firewalls:

- **Firewall Rules** - Each Firewall is initially configured with a standard eHO firewall rule set. Requests for a site-specific customization of firewall rules are treated as Change Request. Additional information regarding the firewall rules can be found in Section 3.1 - eHO Firewall Standard Firewall Rules.
- **Logging** - eHO captures SYSLOG data from each Firewall. Data is stored securely for forensic Security purposes only.

The following configuration parameters have values that are site-specific:

- IP Addressing - eHO assigns unique IP addresses and ranges to each site:
 - One public IP address for the Router/Firewall ONE NETWORK port.
 - A range of unique private IP addresses for local use in addressing workstations/network devices on the LAN. The Firewall dynamically assigns addresses within this range to local devices via DHCP. See Section 2 - IP Address Configuration for additional information.
- Gateway-to-Gateway
 - **VPN Tunnels** - For the Hub & Spoke model only, Hub Sites and Spoke Sites are configured to enable secure communication between each Hub Site and its associated Spoke Sites via gateway-to-gateway IPsec VPN tunnels. See Section 3.2 - Gateway-to-Gateway VPN Tunnels for additional information.

Note: The following Firewall capabilities are **not** used:

DMZ Port - The DMZ port and associated settings are reserved for future use.

3.1 Firewall Constraints

The Firewall is designed to provide optimal performance for up to 10 concurrent IPsec VPN tunnels. This design limit applies to the sum of all concurrent tunnels - including both client-to-gateway and gateway-to-gateway types. The ONE Network Vendor does not support any site that exceeds the design limit of 10 concurrent VPN tunnels. Where a site requires more than 10 concurrent tunnels, the Firewall device will need to be upgraded.

The Firewall is licensed based on a number of users. All licence versions of the Firewall share the same hardware platform and throughput capacity. eHO provides each ONE Network site with the Firewall that best suit their requirements as recorded in the ONE Network Order Form.

3.2 Out of Scope

The following are security areas not addressed by the Firewall:

3.3 *Anti-virus*

Anti-virus protection is the responsibility of the ONE Network Subscriber as per the ONE Network Subscriber Agreement.

3.3.1 Web filtering

Web content filtering is the responsibility of the ONE Network Subscriber as per the ONE Network Subscriber Agreement.

3.3.2 Access Controls

There are no access controls on traffic flowing through gateway-to-gateway VPN tunnels between Hub & Spoke sites.

4.0 IP Address Configuration

4.1 *Firewall ONE NETWORK Port*

- The Firewall ONE Network Port is configured with an eHO-supplied public IP address.
- **LAN IP Range** - eHO assigns IP address ranges to be used by local devices connected to the LAN at each site. These addresses are assigned in contiguous blocks of 64 addresses from a 10.x.x.x IP range. The number of blocks assigned to a site is based on site-specific requirements for LAN IPs recorded in the ONE Network Order Form for the site.
- **Firewall LAN Port** - The lowest address in the site's assigned LAN IP address range is assigned to the LAN port of the Firewall.
- **Static IPs** - Local devices that require static IP addresses (e.g. printers, servers etc.) must be manually configured by the Subscriber's staff or vendor. Static IP addresses are allocated from start of the LAN IP Range assigned to a site.
- **Dynamic IP Block** - The remaining addresses in the assigned range is dynamically assigned by the Firewall to local devices via DHCP.

The Firewall DHCP service also provides each DHCP client with the:

- Default gateway address (which is always the address of the Firewall LAN port)
- Primary and secondary eHO DNS Server addresses.

4.2 *Support for Local DNS resolution*

Sites that require that ability to perform local DNS resolution (such as when Active Directory is used locally) can request on the ONE Network order form that the Firewall not be configured to supply DHCP services. In this case, the site needs to configure their own local DNS and DHCP servers and use the IP address range supplied by eHO. The best results with DNS queries will be achieved with a local DNS server configured to use the DNS servers provided by eHO.

5.0 External Communications Configuration

5.1 *eHO Standard Firewall Rules*

- Allows outbound traffic except Windows file sharing and known malicious traffic. (NetBios over TCP/IP ports 137, 138, 139, 445 and known Trojan ports).
- Blocks all inbound traffic with the following exceptions:
 - Ping is allowed from designated eHO Support locations only.
 - Mail (Port 25), HTTP (Port 80) and HTTPS (Port 443) will be allowed only if requested on the ONE Network Order Form for initial circuit order or ONE Network Change Form after the initial circuit has been installed.

Note: The Firewall does not apply the firewall rules described above to inbound or outbound traffic through VPN tunnels.

Subscriber requests for site-specific changes to the standard firewall rule configuration are reviewed by eHO Privacy and Security for Security Standards compliance and, if approved, performed as a Change Request. When considering requests to open additional ports, you need to keep in mind the following factors:

- The Firewall protects each ONE Network site by restricting traffic allowed in from the ONE Network.
- Each ONE Network site is also protected from Internet traffic by the eHO main firewalls.

Requests to open additional ports are influenced by the intended purpose. For example, if a site wishes to host a web server and provide access only to other users within the ONE Network, that is treated differently than a request to host a web server that would be accessible for all users of the Internet.

eHO may at its discretion update the security profile of the Firewall configuration.

5.2 *Gateway-to-Gateway VPN Tunnels*

For the Hub & Spoke model only, Hub Sites and Spoke Sites are configured to enable secure communication between each Hub Site and its associated Spoke Sites via gateway-to-gateway IPsec VPN tunnels. Spoke-to-Spoke communication is not supported. There are no access controls on the gateway-to-gateway VPN tunnels between Hub & Spokes.

Once a gateway-to-gateway VPN tunnel is established a Hub can access all workstations/devices in the Spoke, and the Spoke can access all workstations/devices at the hub site. Communication between offices occurs via an IP address without DNS or WINS resolution.

Each Firewall is provisioned with a unique Public Key Infrastructure (PKI) certificate that is supplied and managed by eHO. This certificate is used to establish Gateway-to-Gateway tunnels.

6.0 Firewall Configuration Management

6.1 *Change Request Definition and Scope*

After initial configuration of the Firewall, Subscribers may request changes to the following items:

- **LAN IP Address Range** - a request for an increase in the number of LAN IP addresses allocated to their site (in order to accommodate an increase in the number of devices connected to the LAN).
- **Firewall Rules** – a change to the standard firewall rule-set (subject to review and approval by eHO Security)
- **VPN Gateway** - configuration of a new VPN Gateway to enable gateway-to-gateway tunnelling to a new site (e.g. a new Spoke Site), or change or deletion of an existing gateway.

6.2 *Included Services*

The following items are included in the standard ONE Network Managed Service:

- Installation of **Firewall** firmware updates.
- Any change required by the **ONE Network Vendor**.
- Any change required by eHO.

7.0 Appendix A – Glossary

Term	Definition
OMaES	Ontario Medical Association.
ONE Network Access	Extendable Wide Area Network.
ONE Network Access Subscriber	An individual or organization contracts with eHO to receive ONE Network Access services end user who connects to eHO via a ONE Network Access circuit.
ONE Network Access Vendor	A ONE Network Access infrastructure or service support Vendor to eHO.
eHO	eHealth Ontario (formerly Smart Systems for Health Agency).
Firewall	A Firewall Appliance, that assists in basic office network protection through a common protection profile.
Node	A local device that is sending and receiving data through the Firewall. The Firewall count of concurrent nodes includes all devices connected to the LAN port that have sent or received data through the Firewall within the last 24 hours.