

Managed Firewall Service

- 1) Management of Firewall rules based on customer policies and requirements
- 2) Identification of device specific events of interest and significance that require corporate action(s)
- 3) Installation and roll-out of vendor-supplied patches and fixes to the Firewall system itself
- 4) A global, vendor diverse approach to Firewall management so that managed services customers gain great advantage of Neohapsis management capabilities
- 5) Customer determined managed actions based upon corporate requirements, risk mitigation needs and IT governance/compliance requirements

Neohapsis Managed Firewall Service consists of two tiers of service; WATCH and MANAGE:

WATCH

- Customer web Portal Access to the Neohapsis Security Portal
- Service Installation Management
- Device Incident Management (Validation, Notification, and Escalation)
- Trend Reporting

MANAGE - All the features of WATCH, plus:

- Notification & Escalation of device events and downtime within 15 minutes of detection
- Device Problem Management (Error Control, Root Cause Analysis)
- Device Change Management
- Device Configuration Management
- Device Release Management
- Device Patch Management and Performance Review

Service Components Details

Within Neohapsis Firewall Service, there are several

service components.

WATCH Service Level

Service Activation:

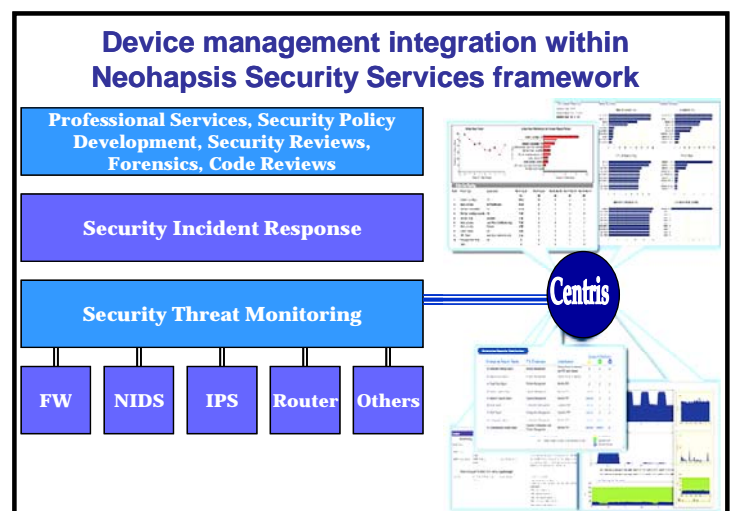
During the Service Activation stage Neohapsis may do the following, depending on the specific service purchased by the Client.

- Required check to make sure that the Firewall system is up and running
- Run a test to check the NOC's ability to see a Firewall system failure

Additionally, for clients with the MANAGE Service Level, the Client will provide Neohapsis with exclusive administrative privileges on the specific devices that will be managed by Neohapsis.

Device Uptime and Health Monitoring:

All of Neohapsis firewall services include uptime and health monitoring. The NOC monitors these two variables through periodic polling of the firewall device. If a response is not received, an automatic alert is sent to the NOC and a ticket is generated. The ticket is forwarded to a NOC analyst who then notifies the Client that the firewall is down. If the customer has purchased the MANAGE service option, in addition to notifying the Client, the NOC analyst will identify the source of the problem. If the problem lies with the firewall, the



analyst will troubleshoot the issue until the root cause has been identified. If on-site work is required, Neohapsis will work with the Client's designated point of contact via phone to address any device related problems. If Neohapsis determines that the problem is due to a client side issue, it will stop all troubleshooting work. If the Client requests further assistance from Neohapsis, Neohapsis will do so for an additional fee.

Customer Portal and Reporting:

Device statistics and reporting are available from Neohapsis Security portal.

MANAGE Service Level

Upgrade and Patch Maintenance:

The Client is responsible for maintaining valid support and maintenance agreements with the vendor. Neohapsis will monitor all vendors represented on Neohapsis approved platforms list for release activities related to software patches and upgrades. As security related software patches and upgrades are released by the third-party product vendors, Neohapsis will assess the applicability of the release to the Client's environment. Neohapsis will work with the Client to schedule any necessary remote upgrades. Software upgrades will be implemented by Neohapsis as part of the selected service, so long as the following conditions apply:

- The upgrade can be performed remotely either independently or with a minimal amount of onsite assistance by the Designated Client Network Engineer
- The upgrade does not require a change to underlying hardware on which the software is running

A single upgrade or patch should not require more than 2 hours of Neohapsis' time. Neohapsis will bill the Client for all work beyond the allocated 2 hours. If the upgrade requires any additional licensing or maintenance fees, the Client will be responsible for these fees. In cases where a replacement firewall is requested during the period of the upgrade or patch maintenance work, the client will be responsible for providing the replacement equipment.

In cases where support for a particular product or product version is being discontinued by the vendor or by Neohapsis, Neohapsis will communicate new

platform migration options. In order to be assured of uninterrupted service, the customer must complete the migration process within 60 days. The Client will bear any costs relating to procuring new hardware or components and to re-provisioning any devices. SLAs do not apply during maintenance work. Service levels cannot be guaranteed if the Client does not make the changes required by Neohapsis or if the Client prevents Neohapsis from making the changes it deems necessary for continued service.

Change Management:

Neohapsis will provide a certain number of firewall policy and configuration changes per month as specified in the package descriptions. The types of firewall policy and configuration changes considered in-scope are described in the definitions section. All other changes are considered out of scope and may be implemented on a time and materials basis.

The Client may submit a standard change request to Neohapsis via telephone or the Client Portal. The Client will be prompted to provide a detailed description of the required change. Neohapsis will validate that the rule change has been requested by an authorized person and will contact the Client to clarify requests as needed.

Neohapsis will also maintain a backup copy of the firewall configuration for recovery purposes in the event of a significant hardware failure.

Raw Log File Transfer:

Certain Neohapsis firewall service packages include raw log file transfer. For firewalls that generate Syslog log files, Neohapsis can configure the firewall to send the raw log data to a location inside the customer's network on a regular basis. If additional hardware and/or software are required, the Client will bear the cost and is responsible for managing it.

Other Services:

Any other services are out-of-scope. As described in Overview, upon request, Neohapsis may provide out-of-scope support on a time and materials basis. Examples of out-of-scope support related to the firewall service that may be requested include the following:

- On-site installation and provisioning of firewall
- Integration of additional products that the

Client has chosen not to have managed by Neohapsis

- Custom analysis reports
- Any change requests not specified as covered under Neohapsis change request service
- Configuration of any VPN tunnel end point that is not terminated on a Neohapsis-managed device
- Customized policy for security event monitoring

Customer Requirements:

- Customer will provide the firewall as well as vendor maintenance contract for the firewall
- Customer will provide internal technical points of contact for configuration issues, incident response actions and maintenance-related issues
- Customer will also provide a current network topology, asset inventory and network data flow documentation to assist in alert validation and firewall configuration.

Services Not Included:

- Firewall hardware and /or support contract
- Permanent archival storage of log files
- Forensic services (Neohapsis can provide these services separately)

Add On Options

Design Services:

- Review security policy, if in place, to identify any unique requirements for Firewall deployment
- Review any other operational documentation that includes security and access controls
- Review network architecture (diagrams provided by client)
- Review connections with other networks and the Internet

High Availability:

As an optional service upgrade, Neohapsis offers a High Availability solution for firewalls that support High Availability natively. This solution involves a firewall pair deployed in an active/standby configuration. In the event that the active firewall fails, the standby firewall is engaged to ensure uninterrupted service. Neohapsis may support other high availability options on a case-by-case basis.

Site-to-Site VPN Management:

Certain Neohapsis firewall service packages include VPN management of connections between two firewalls from the same vendor and running on the same platform. At least one firewall must be managed by Neohapsis. Neohapsis may manage a VPN connection between two firewalls not running on the same platform on a case-by-case basis for an additional fee. Neohapsis will monitor for uptime, troubleshoot in the event of an outage and make required configuration changes.

For Client's that want Neohapsis to manage more site-to-site VPN connections than are included in their Work order, Neohapsis will do so for an additional charge.

Client-to-Site VPNs:

As an optional service upgrade, Neohapsis can manage client-to-site VPNs. This involves troubleshoot and make required configuration changes to the firewall to support client-to-site VPNs and adding, deleting and modifying user profiles. Neohapsis will provide troubleshooting support only to the Client designated Primary Technical Contact. For problems with individual connections, Neohapsis will verify appropriate configuration of the firewall, but will not provide any support for issues with the user's software or the user's firewall or NAT. The customer will continue to do user management so they can add, delete or modify users at their leisure.

Firewall Policy Rule and Configuration Change

The following defines what Neohapsis considers to be one policy change:

- Adding, deleting or modifying up to two individual (NAT/Rule/Route) per day within the firewall

Any change request that is not specifically listed above may be completed by Neohapsis on a time and materials basis. The following are examples of changes that are not considered Policy Changes but can be requested on a time and materials basis:

- Ongoing software or hardware upgrades
- Physical or logical relocation of devices

- Modifications to the network topology around or into the device
- Substantial changes to the feature set used by the firewall
- Neohapsis reserves the right to determine, within its reasonable discretion, if the change falls within the scope of the Client's service

Other Complementary Neohapsis Services

Neohapsis offer a selection of complementary services

Neohapsis Network IDS/IPS Service

The Neohapsis Network IDS/IPS Service provides monitoring and management for customer Network IDS/IPS devices.

Neohapsis Security Threat Monitoring Service

Active 24x7 monitoring and filtering of security events generated from a wide variety of supported platforms,

correlated and validated by the Neohapsis NOC. The Neohapsis Security Threat Monitoring service allows genuine threats to be identified and escalated to the correct response teams.

Neohapsis Security Incident Response Service

The Neohapsis Security Incident Response Service provides the customer with access to highly trained Neohapsis personnel that can be brought in at short notice to provide guidance and support when a significant Security Incident occurs.

Neohapsis Professional Services

A wide range of review and process services are available from Neohapsis Professional Services including Network Security Reviews, Incident Response Policy development, Application code security reviews and device Forensics.

ABOUT NEOHAPSIS

Founded in 1997, Neohapsis is a leader in delivering managed risk services. Neohapsis is the first Managed Risk Services Provider (MRSP) to expertly align organizations' unique risk profiles with a new breed of managed and professional services designed to mitigate corporate and personal liability. Our holistic approach to enterprise risk management blends security, information technology, and operations management with an innovative set of services that ensures ongoing confidentiality, integrity, availability, and efficiency.

Neohapsis provides high-quality, in-depth independent security consulting, forensic services, and product testing. Neohapsis' experts deliver specialized services in information risk management, application security, network and endpoint security, security product testing, and digital forensics. Neohapsis Lab, a highly respected independent IT product testing facility, backs this consulting expertise.

Neohapsis also offers a full spectrum of managed services, delivered by our team of world-class security and risk management experts who have defined much of what is considered standard practice in the industry. This depth of expertise enables Neohapsis to optimize our approach in addressing each of our clients' unique needs, especially in times of crisis, and to mentor senior managers responsible for managing information risk. Neohapsis' clients include some of the world's most well respected organizations, encompassing a wide range of industry sectors. To learn more, visit Neohapsis at: www.neohapsis.com.

© 2002, 2003, 2004, 2006, 2007 by Neohapsis, Inc. All rights reserved. Neohapsis reserves the right to change or modify any information contained herein without notice. Reproduction of this document in any form without prior written permission is strictly forbidden. Centris and the Centris logo are trademarks of Neohapsis. All other products or services referenced herein are the trademarks or service marks of their respective companies or organizations.

